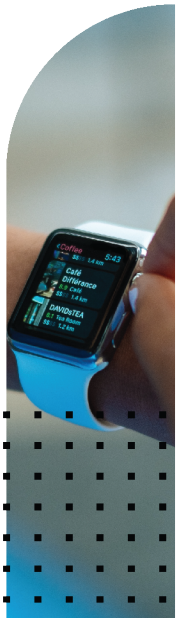
Cookbook

FortiAuthenticator 6.3.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 7, 2021
FortiAuthenticator 6.3.0 Cookbook
23-630-690320-20210607

TABLE OF CONTENTS

Change Log

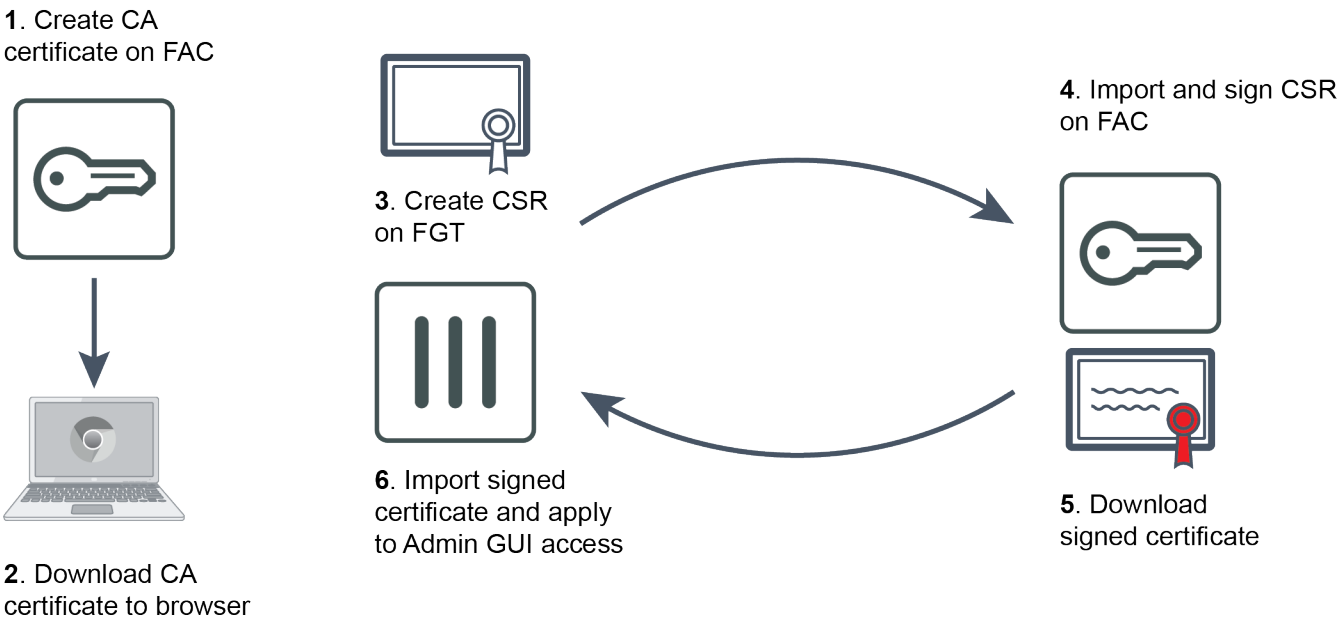
Date	Change Description
2021-04-22	Initial release.
2021-06-07	Updated Configuring FortiAuthenticator on page 194.

Certificate management

This section describes managing certificates with the FortiAuthenticator device.

FortiAuthenticator can act as a certificate authority (CA) for the creation and signing of X.509 certificates, such as server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPsec VPN.

FortiAuthenticator as a Certificate Authority



For this recipe, you will configure the FortiAuthenticator as a Certificate Authority (CA). This will allow the FortiAuthenticator to sign certificates that the FortiGate will use to secure administrator GUI access.

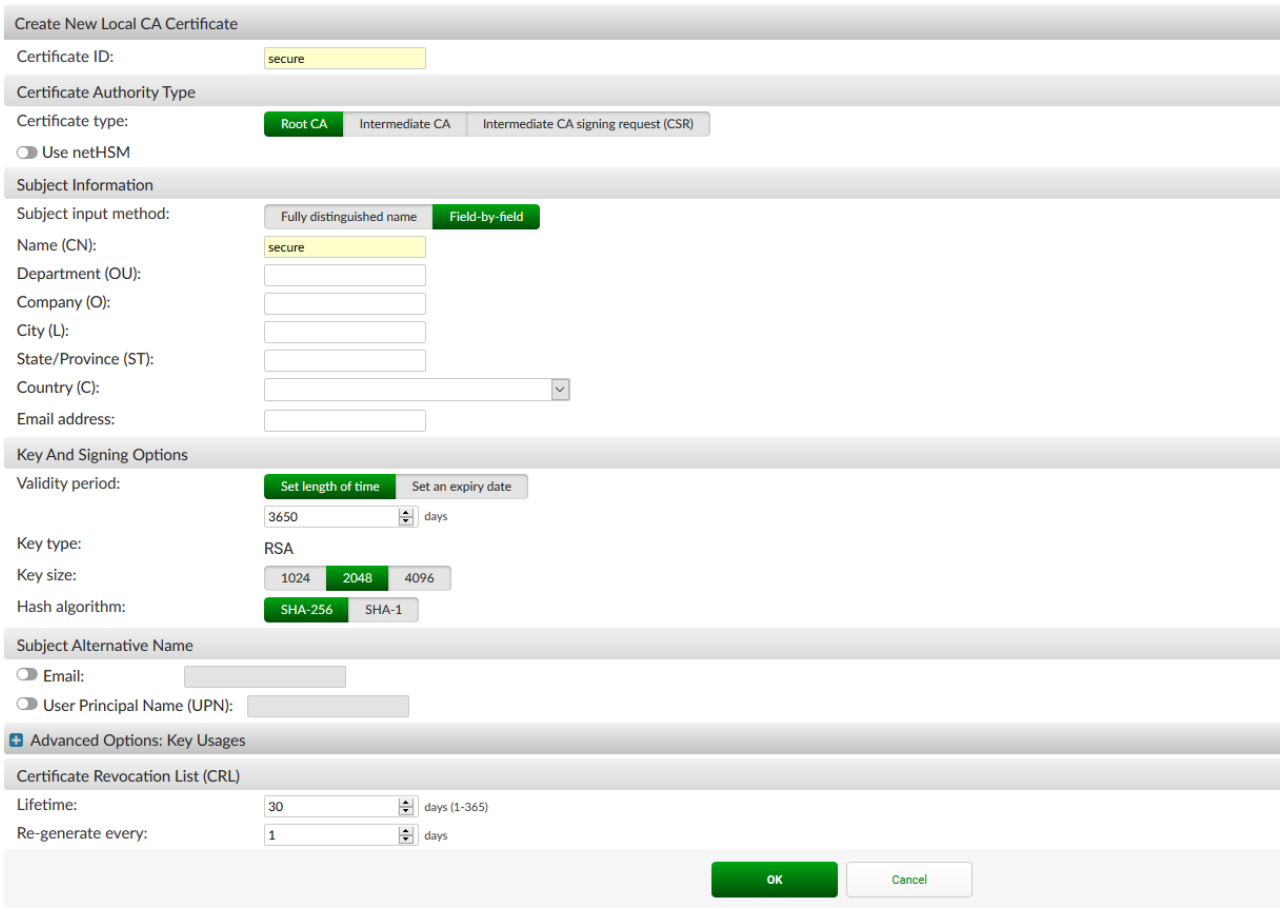
This scenario includes creating a certificate request on the FortiGate, downloading the certificate to the network's computers, and then importing it to the FortiAuthenticator. You will sign the certificate with the FortiAuthenticator's own certificate, then download and import the signed certificate back to the FortiGate.

The process of downloading the certificate to the network's computers will depend on which web browser you use. Internet Explorer and Chrome use one certificate store, while Firefox uses another. This configuration includes both methods.

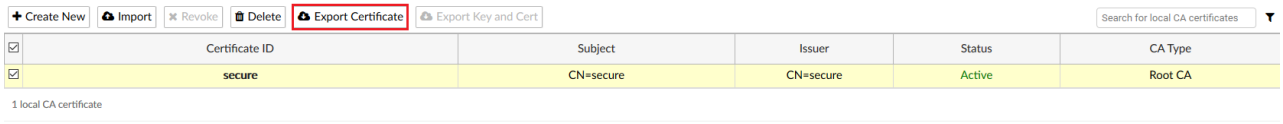
Creating a new CA on the FortiAuthenticator

To create a new CA:

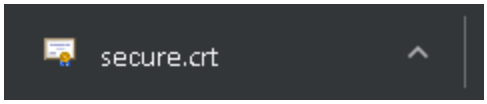
1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and create a new CA. Enter a *Certificate ID*, select *Root CA certificate*, and configure the key options as shown in the example.



2. Once created, highlight the certificate and select *Export Certificate*.



This will save a *.crt* file to your local drive.

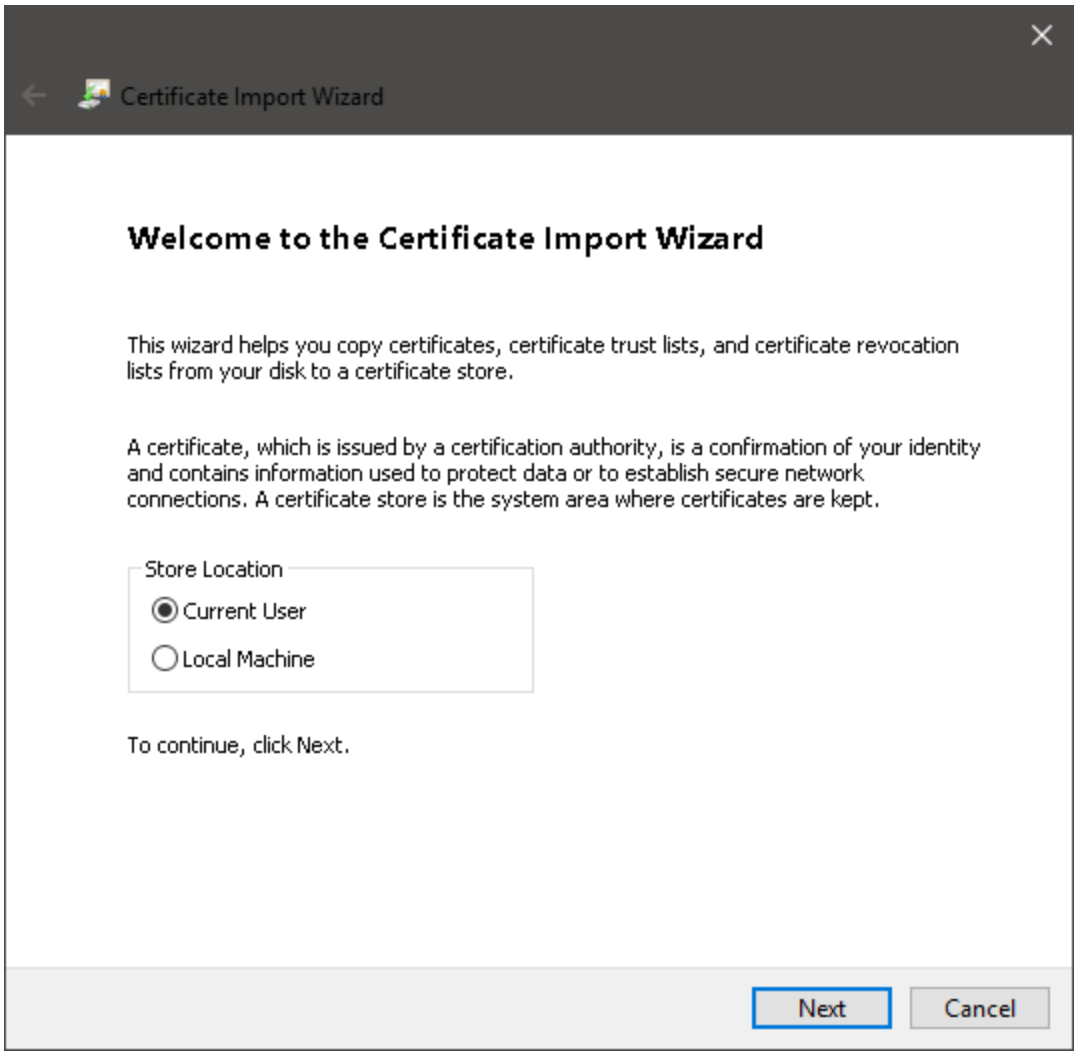


Installing the CA on the network

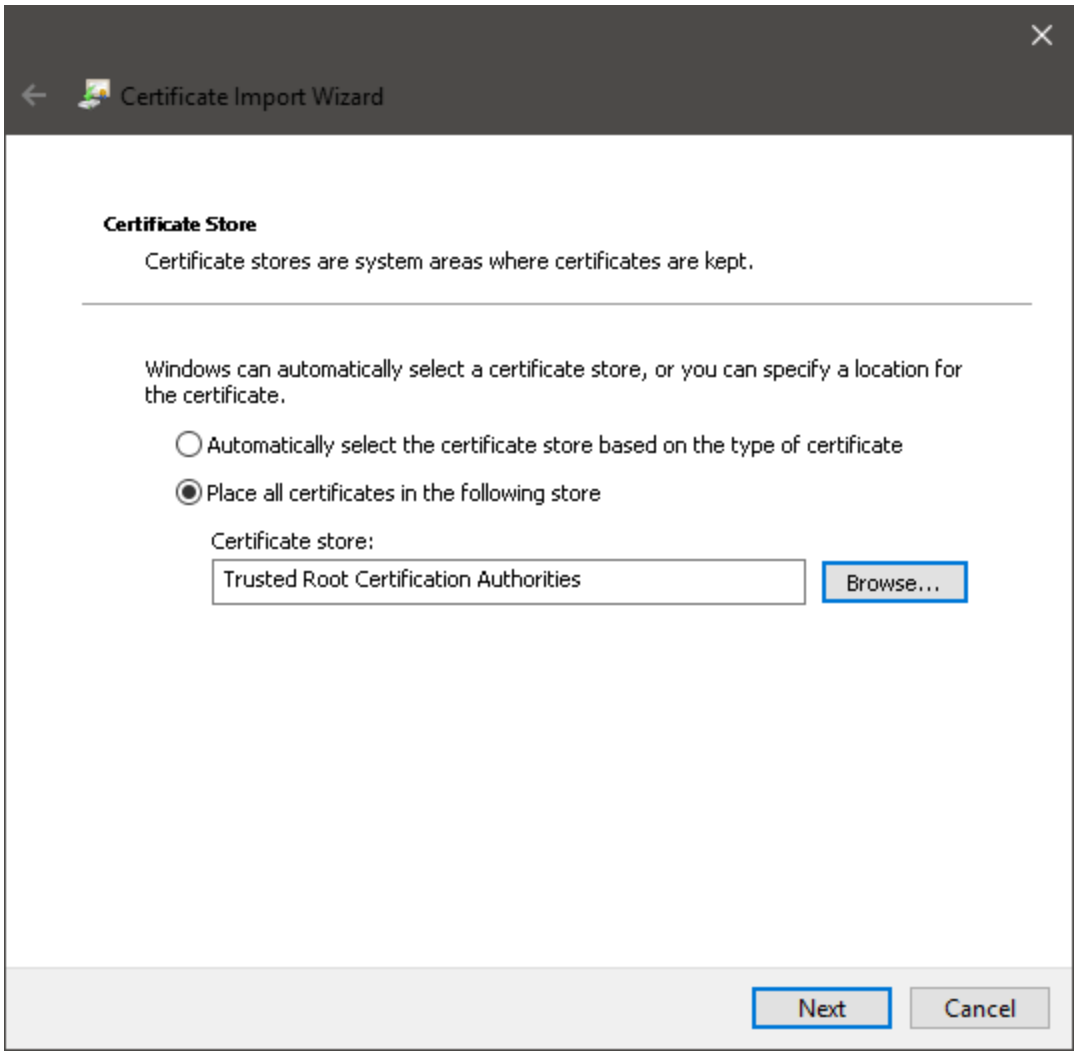
The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

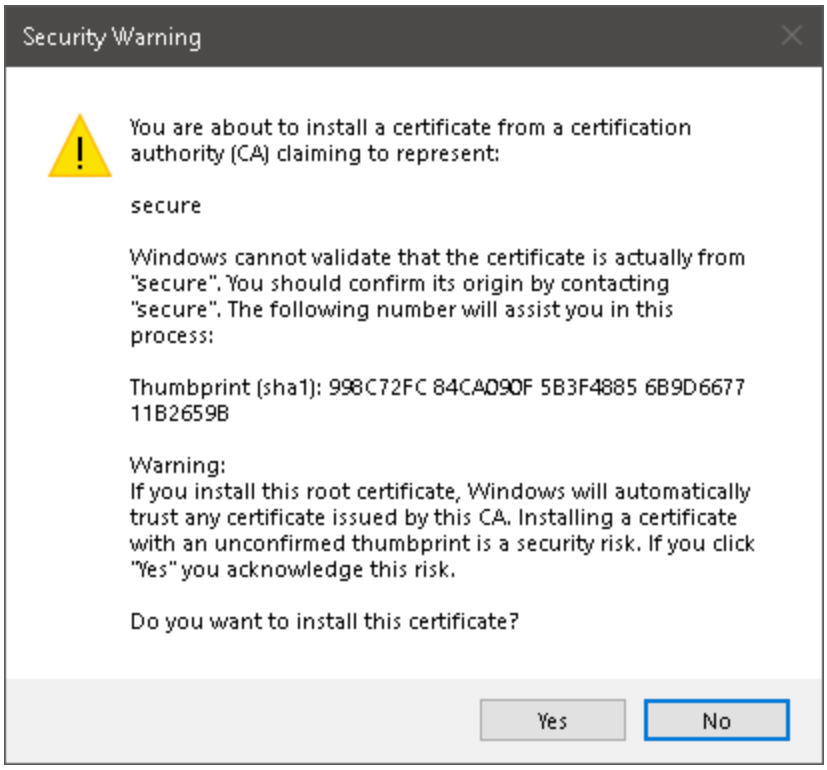
1. In Windows Explorer, right-click on the certificate and select *Install Certificate*. Open the certificate and follow the *Certificate Import Wizard*.



2. Make sure to place the certificate in the *Trusted Root Certification Authorities* store.

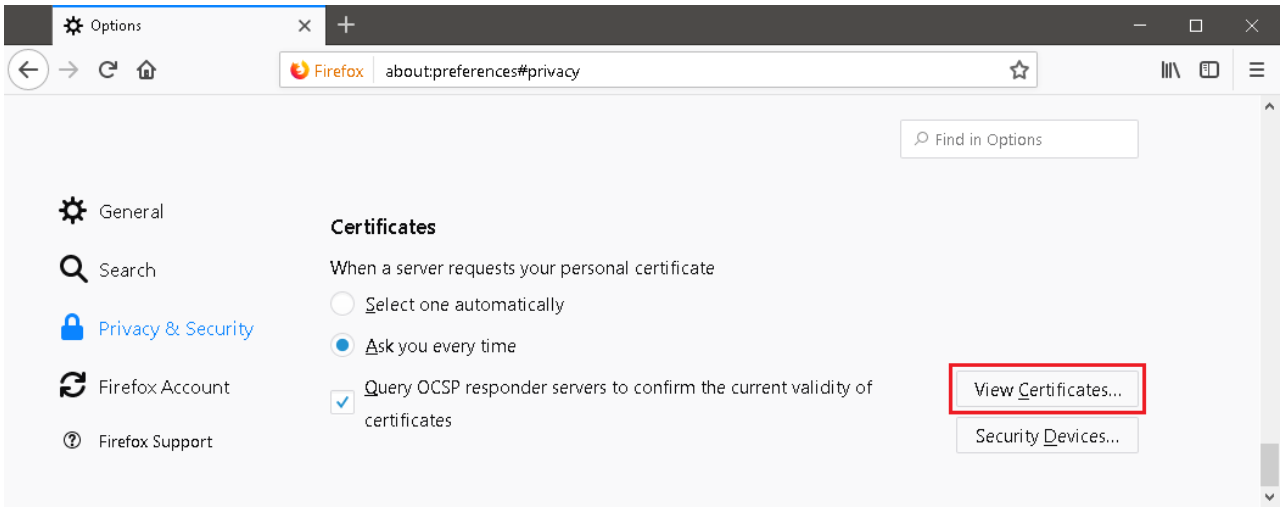


3. Finish the Wizard and select *Yes* to confirm and install the certificate.

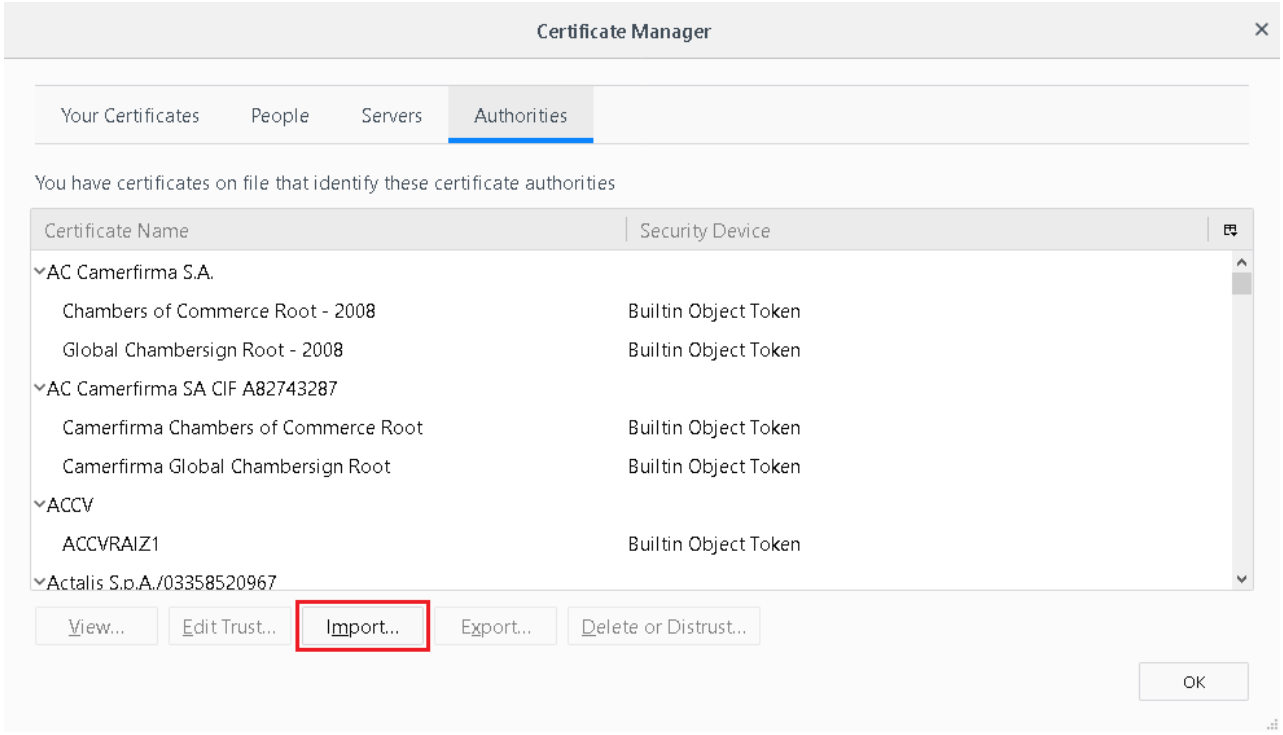


Firefox

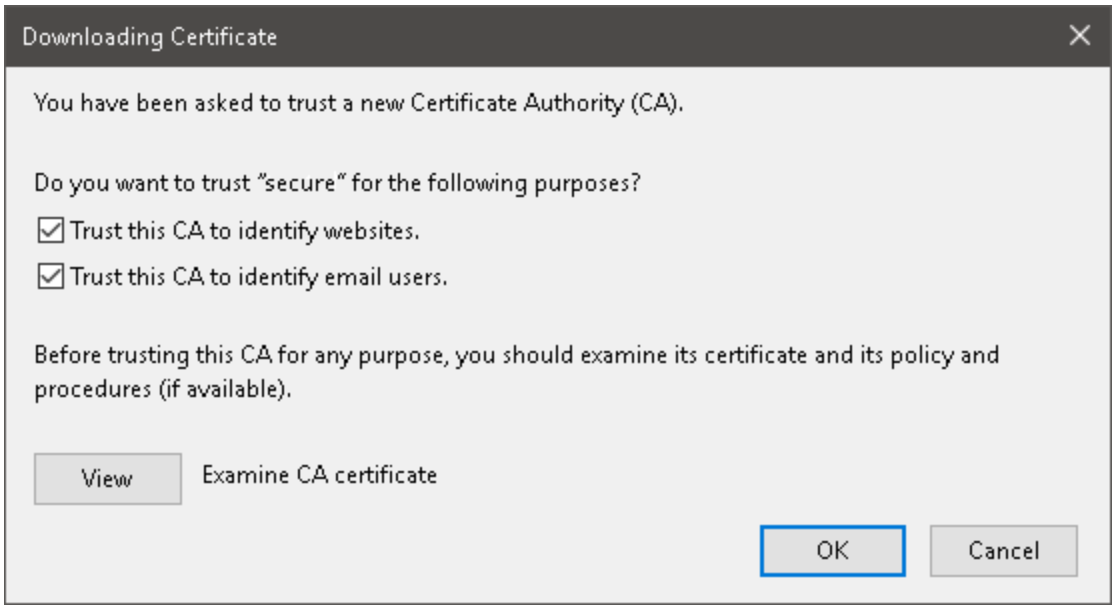
1. In the web browser, go to *Options* > *Privacy & Security* > *Certificates*, and select *View Certificates*.



2. In the *Authorities* tab, select *Import*.



3. Find and open the root certificate.
   You will be asked what purposes the certificate will be trusted to identify. Select all options and select *OK*.

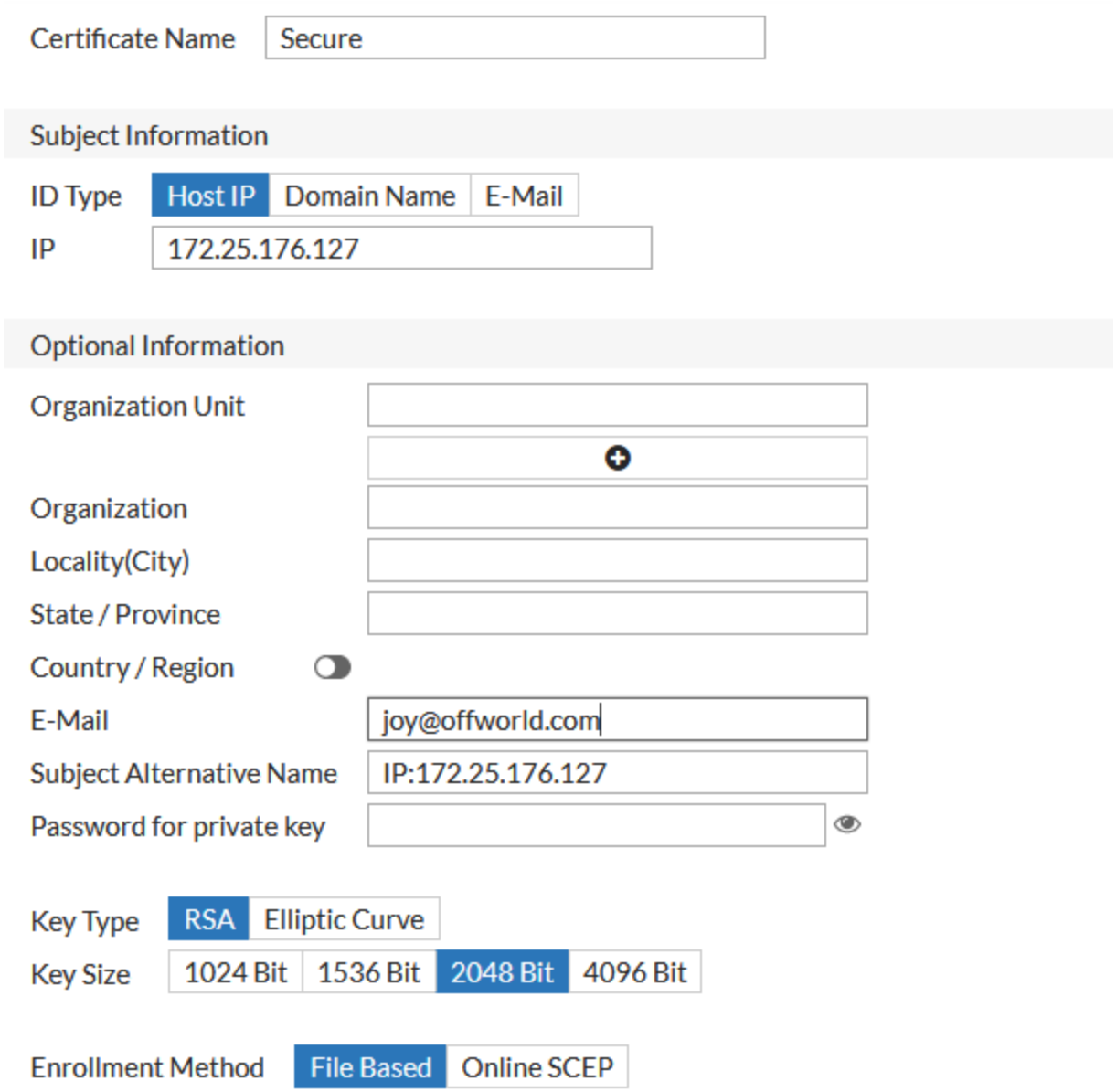


Creating a CSR on the FortiGate

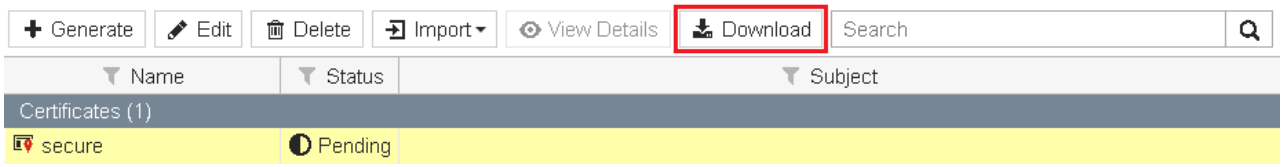
To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.

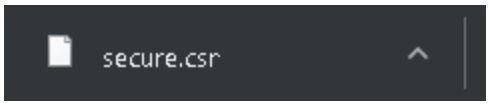
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



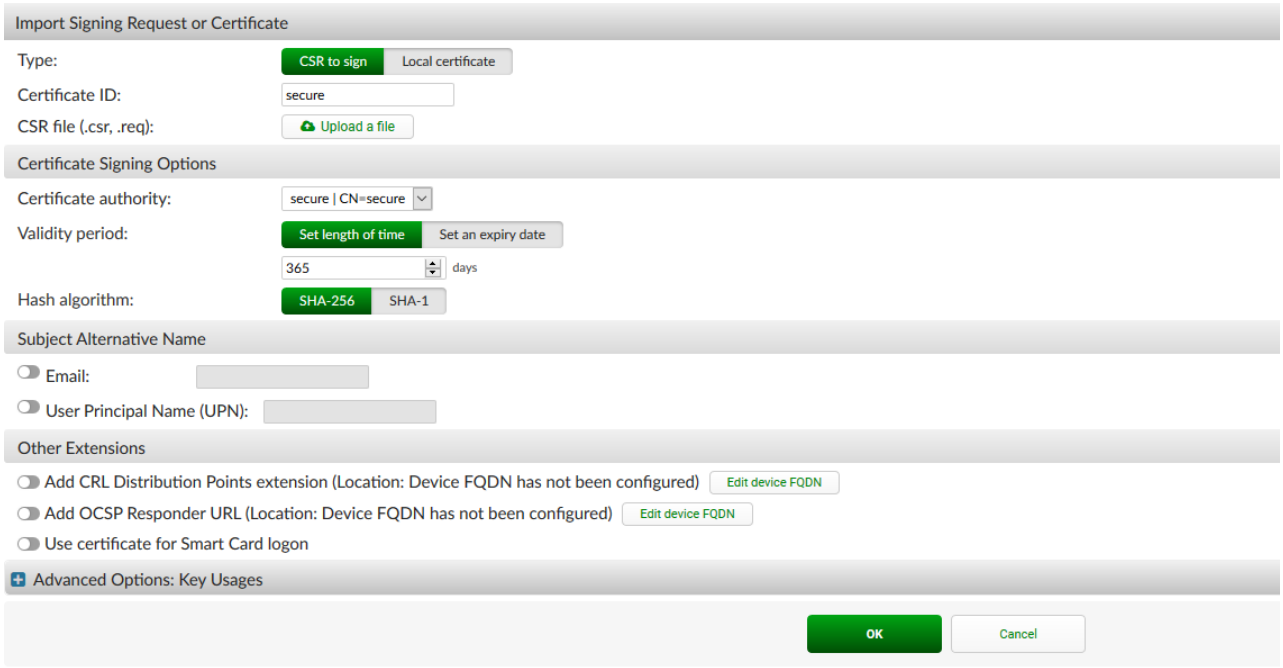
This will save a **.csr** file to your local drive.



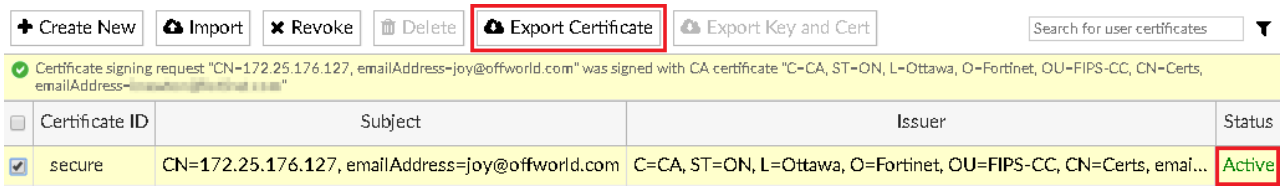
Importing and signing the CSR on the FortiAuthenticator

To import and sign the CSR:

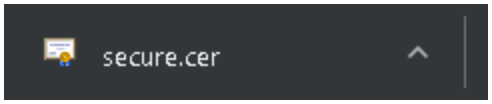
1. Back on the FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users* and import the *.csr* certificate created earlier.
   Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm* to *SHA-256*, as configured earlier.



2. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, with a *Status* of *Active*. Highlight the certificate and select *Export Certificate*.



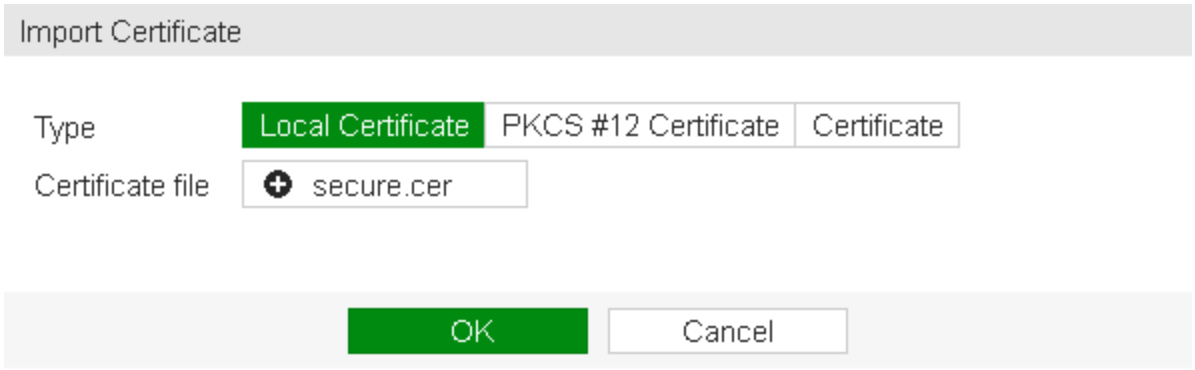
This will save a **.cer** file to your local drive.



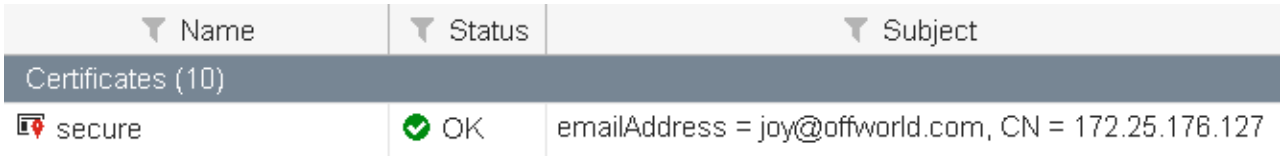
Importing the local certificate to the FortiGate

To import the local certificate:

1. Back on the FortiGate, go to *System* > *Certificates*, and select *Local Certificate* from the *Import* dropdown menu. Browse to the *.cer* certificate, and select *OK*.



You should now see that the certificate's *Status* has changed from *Pending* to *OK*. You may have to refresh your page to see the status change.

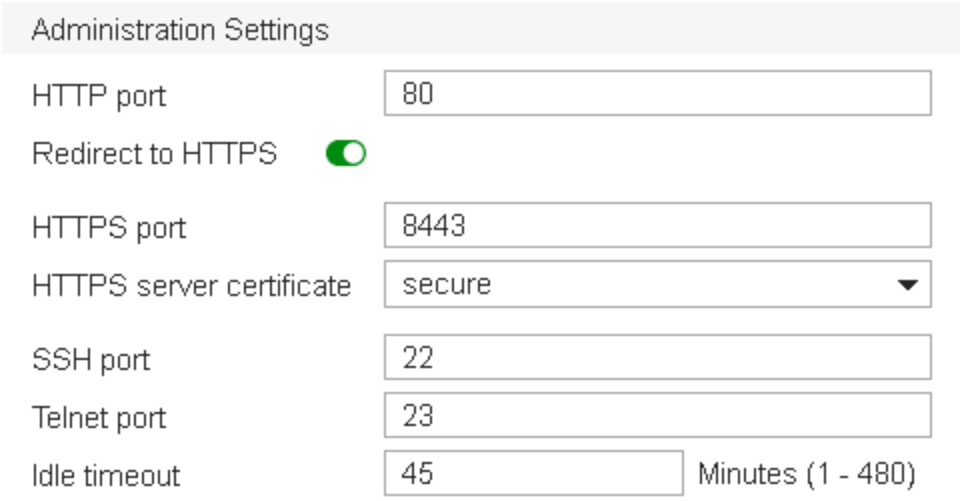


Configuring the certificate for the GUI

To configure the certificate:

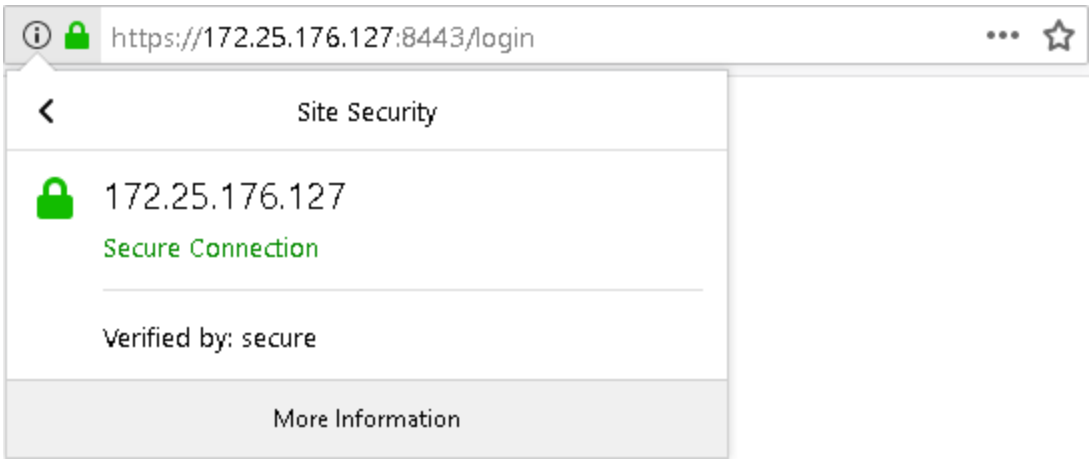
1. On the FortiGate, go to *System* > *Settings*.
   Under *Administration Settings*, set *HTTPS server certificate* to the certificate created/signed earlier, then select

Apply.

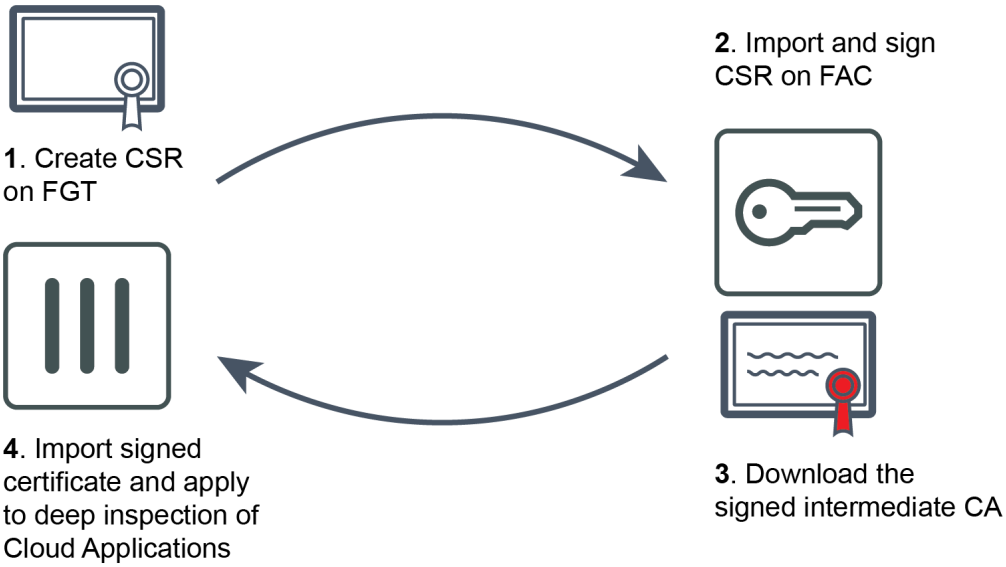


Results

Close and reopen your browser, and go to the FortiGate admin login page. If you click on the lock icon next to the address bar, you should see that the certificate has been signed and verified by the FortiAuthenticator. As a result, no certificate errors will appear.



FortiAuthenticator certificate with SSL inspection



For this recipe, you will create a certificate on the FortiGate, have it signed on the FortiAuthenticator, and configure the FortiGate so that the certificate can be used for SSL deep inspection of HTTPS traffic.

Note that, for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see FortiAuthenticator as a Certificate Authority.

This scenario includes creating a certificate signing request (CSR), signing the certificate on the FortiAuthenticator, and downloading the signed certificate back to the FortiGate. You will then create an *SSL/SSH Inspection* profile for full SSL inspection, add the certificate created to the profile, and apply the profile to the policy allowing Internet access.

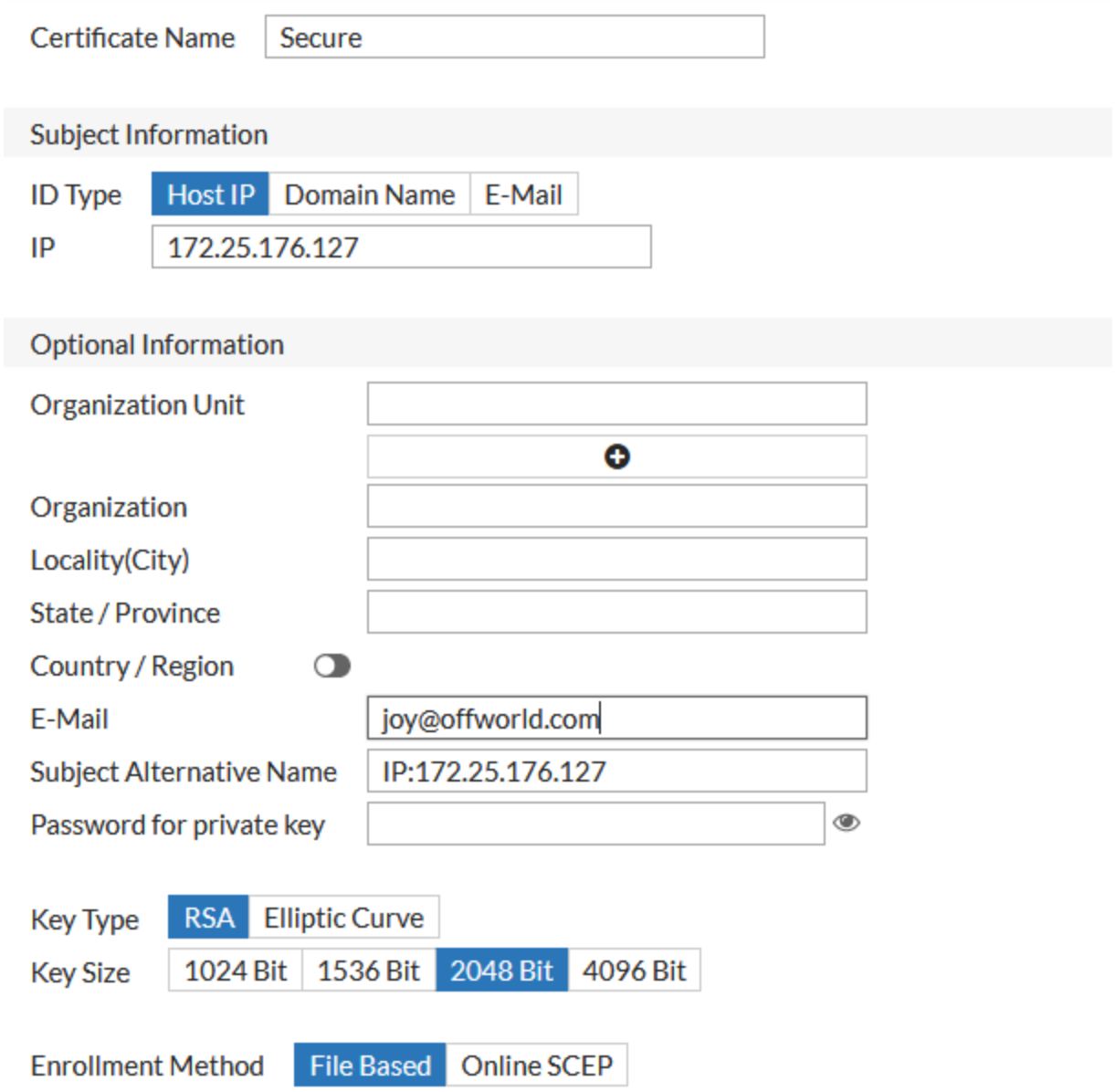
As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

Creating a CSR on the FortiGate

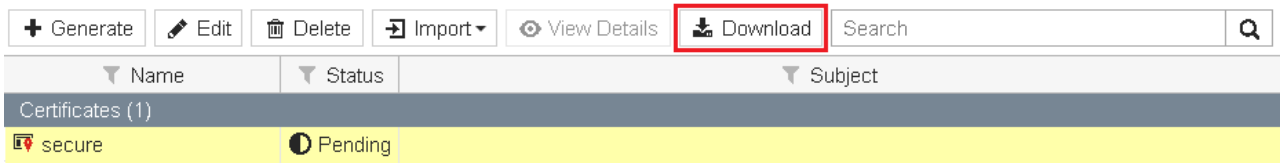
To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.

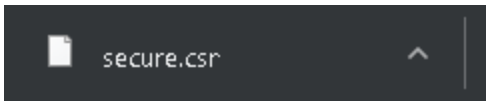
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



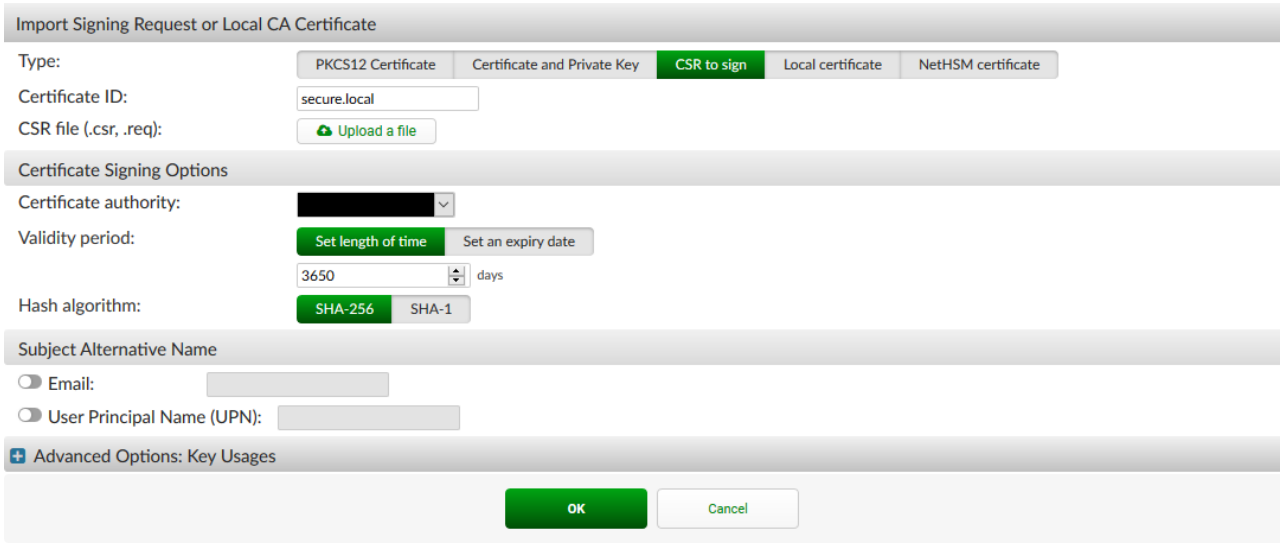
This will save a **.csr** file to your local drive.



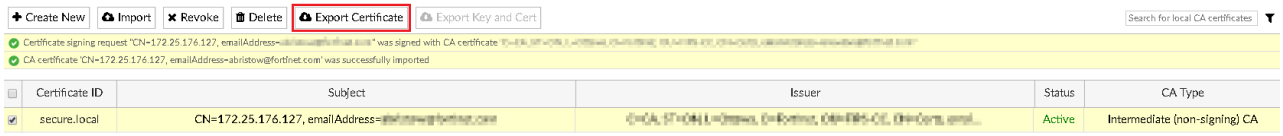
Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

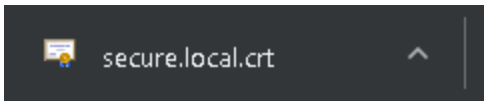
1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file. Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm* to *SHA-256*.



2. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, showing a *Status* of *Active*, and with the *CA Type* of *Intermediate (non-signing) CA*. Highlight the certificate and select *Export Certificate*.



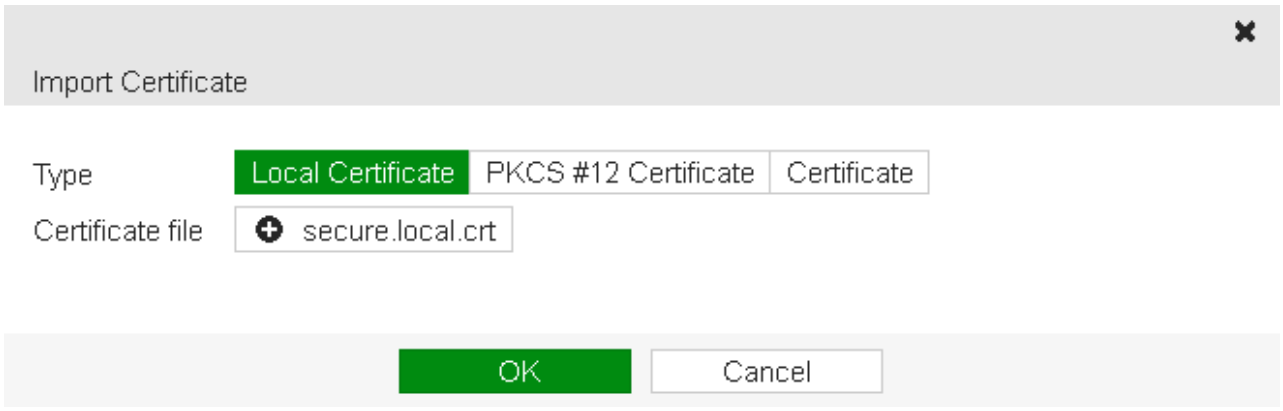
This will save a *.crt* file to your local drive.



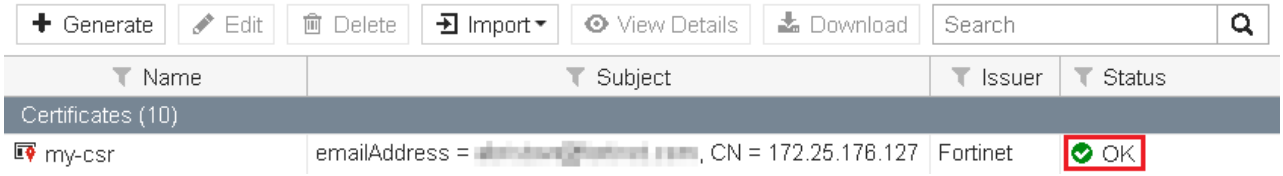
Importing the signed certificate on the FortiGate

To import the signed certificate:

1. Back on the FortiGate, go to *System* > *Certificates*, and select *Import* > *Local Certificate*. Browse to the CRT file and select *OK*.



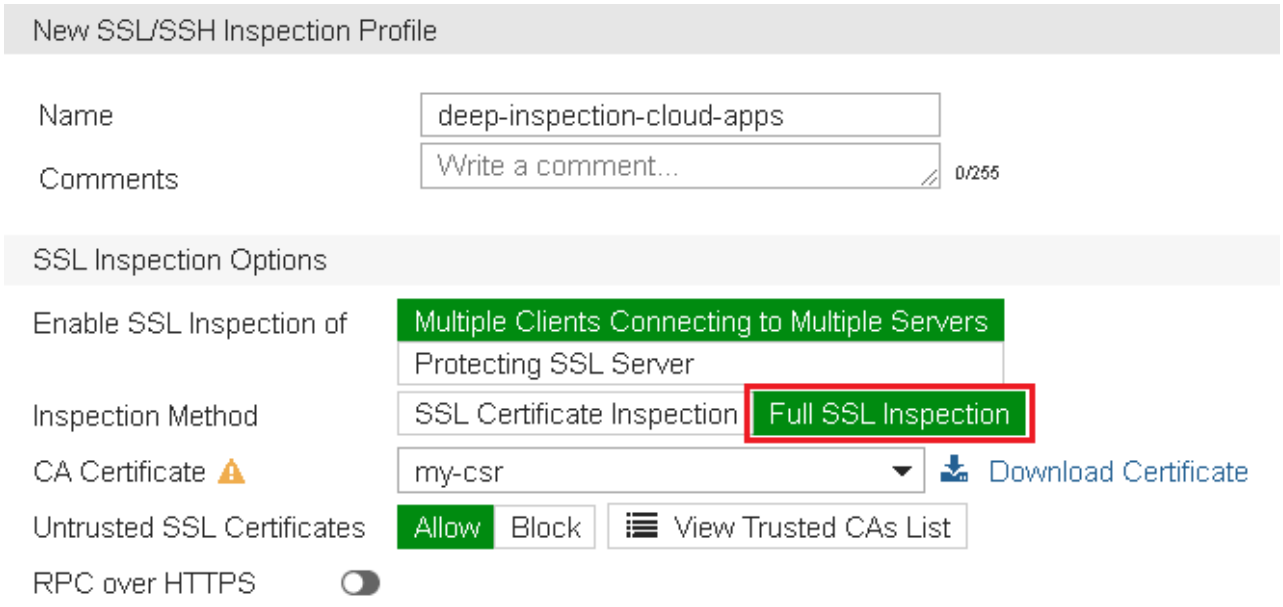
2. You should now see that the certificate has a *Status* of *OK*.



Configuring full SSL inspection

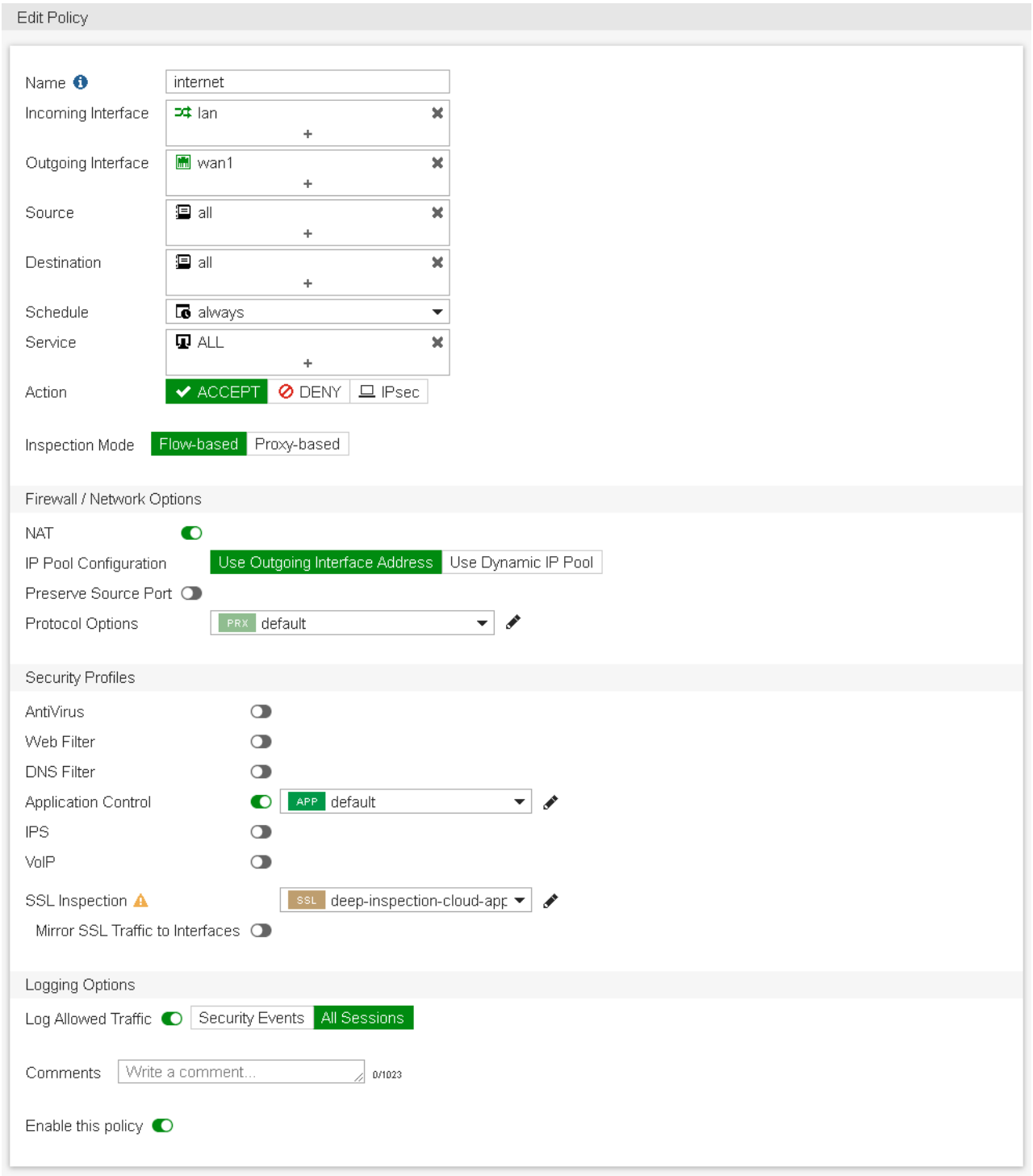
To configure full SSL inspection:

1. Go to *Security Profiles* > *SSL/SSH Inspection*, and create a new profile.
   Enter a *Name*, select the certificate from the *CA Certificate* dropdown menu, and make sure *Inspection Method* is set to *Full SSL Inspection*.



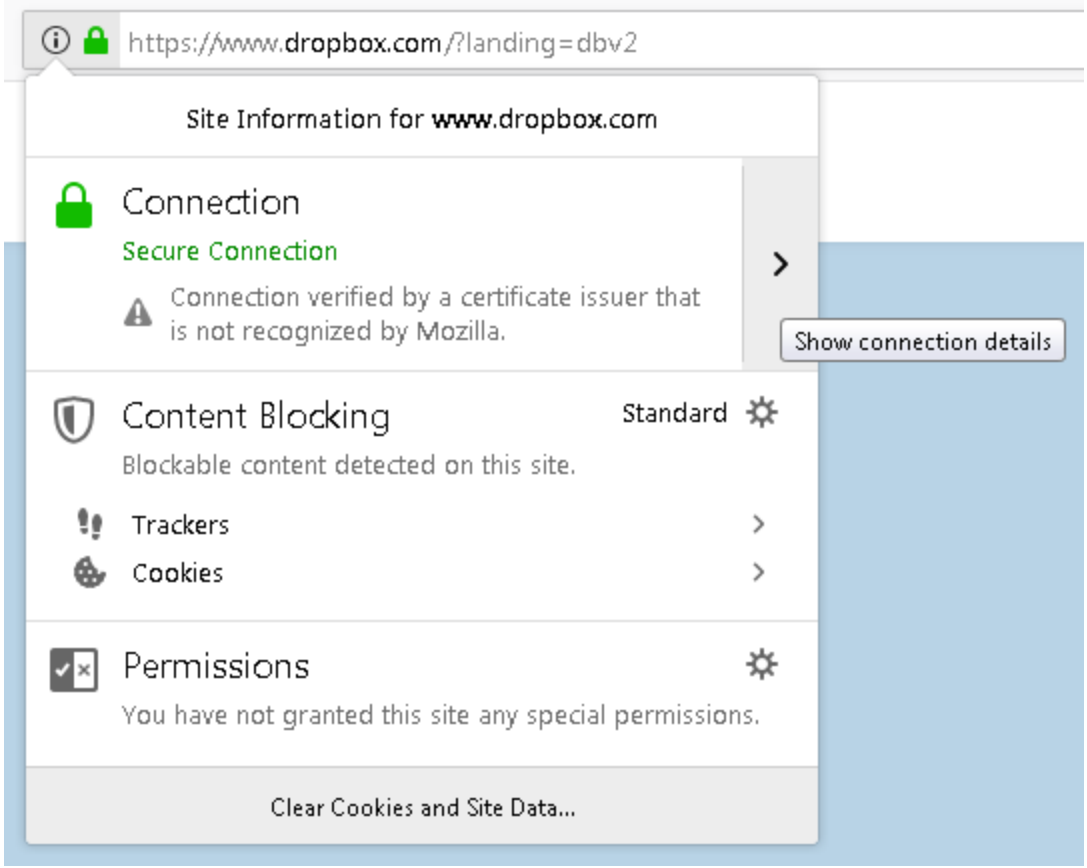
2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.

3. Next go to *Policy & Objects* > *IPv4 Policy* and edit the policy that allows Internet access.
   Under *Security Profiles*, enable *SSL/SSH Inspection* and select the custom profile created earlier.
   Enable *Application Control* and set it to *default*.



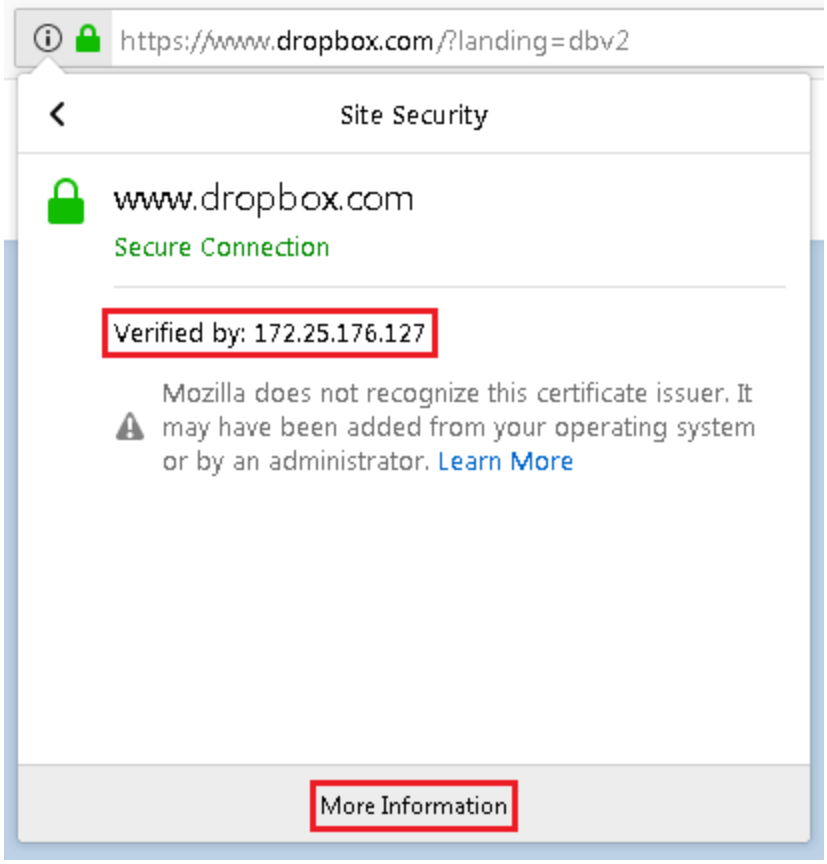
Results

1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, `https://www.dropbox.com`).
   Click on the lock icon next to the address bar and click *Show connection details*.

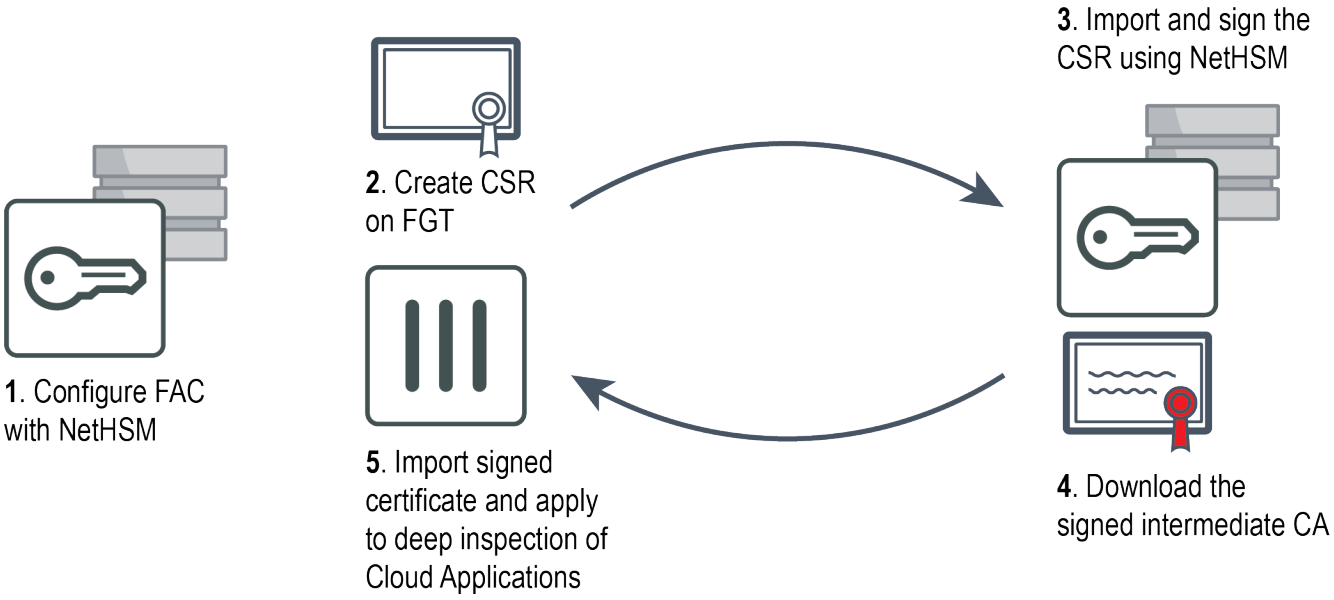


2. You should now see that the certificate from the FortiGate (`172.25.176.127`) has signed and verified access to the site. As a result, no certificate errors will appear.

Optionally select *More Information*.



FortiAuthenticator certificate with SSL inspection using an HSM



For this recipe, you will create a certificate on the FortiGate, have it signed on a FortiAuthenticator with a configured HSM server, and configure the FortiGate so that the certificate can be used for SSL deep inspection of HTTPS traffic. This example uses the Safenet Luna V7 HSM.

To set up the certificate with SSL inspection using an HSM:

1. Configuring the NetHSM profile on FortiAuthenticator on page 25
2. Creating a local CA certificate using an HSM server on page 26
3. Creating a CSR on the FortiGate on page 27
4. Creating an Intermediate CA on the FortiAuthenticator on page 28
5. Importing the signed certificate on the FortiGate on page 29
6. Configuring full SSL inspection on page 29
7. Results on page 32

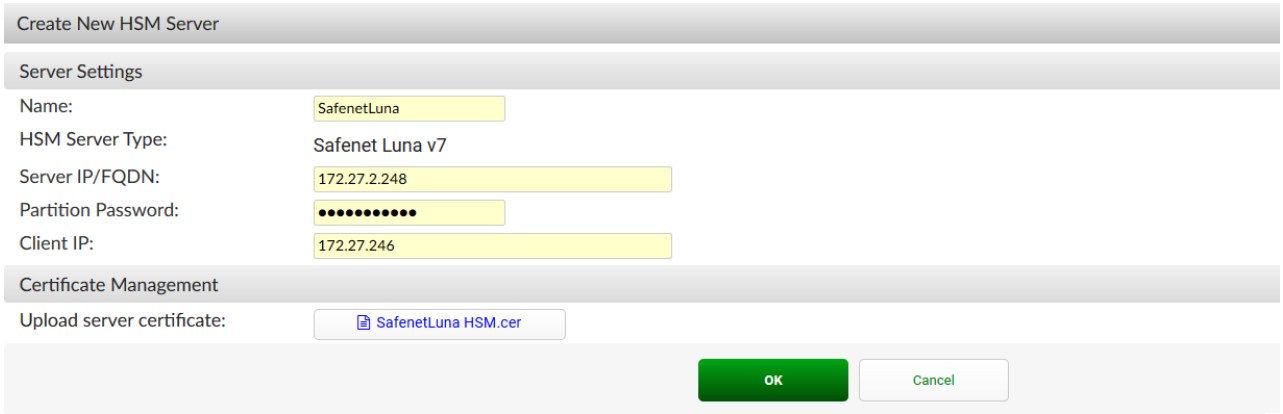
In order for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see Creating a local CA certificate using an HSM server on page 26 and FortiAuthenticator as a Certificate Authority.

As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

Configuring the NetHSM profile on FortiAuthenticator

To configure a new the Safenet Luna HSM server:

1. In FortiAuthenticator, go to *System* > *Administration* > *NetHSMs*, and click *Create New*.
2. In the *Create New HSM Server* window, configure the following:



Name	Enter a name for the HSM server.
Server IP/FQDN	Enter the IP address or FQDN of the HSM server to which the FortiAuthenticator will connect.
Partition Password	Enter the key partition password from the HSM server.
Client IP	Enter the address of the FortiAuthenticator interface that the HSM will see.
Upload server certificate	Click *Upload server certificate* to select the certificate from your HSM.

3. Click *OK* to complete the setup.

To authorize FortiAuthenticator as a Safenet Luna HSM client:

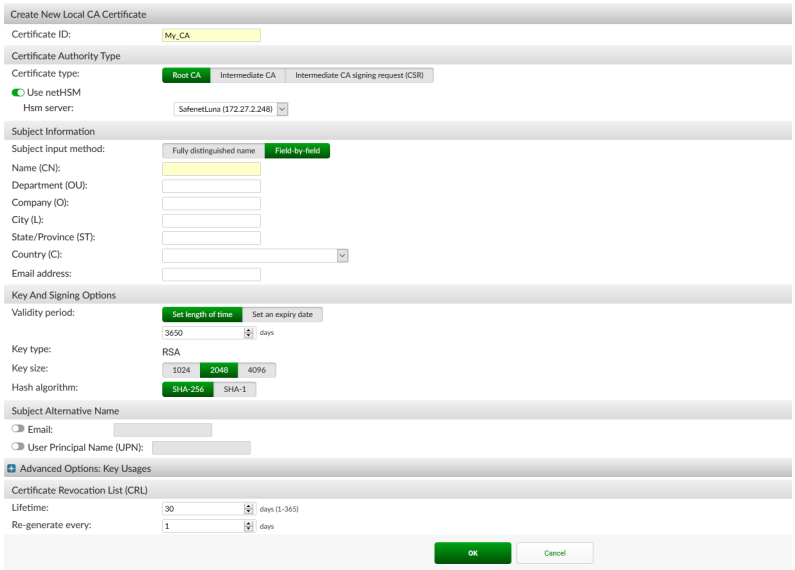
1. Make sure the FortiAuthenticator client certificate uses the `<FAC IP>.pem` naming convention. For example: `172.16.68.47.pem`
2. Upload the FortiAuthenticator client certificate to Safenet Luna HSM using SCP transfer.
   ```
   scp [certificate filename] admin@[HSM address]:
   ```
3. Use SSH to connect to the HSM, then register your FortiAuthenticator, and associate it with a partition.
   ```
   ssh -1 admin [HSM address]
   client register -c [client name] -ip [client address]
   client assignpartition -c [client name] -p [partition name]
   ```
4. Confirm the status of the NetHSM client. For example:
   ```
   client show -c my_fac
      ClientID: my_fac
      IPAddress: 172.16.68.47
      Partitions: my_partition
   ```

Creating a local CA certificate using an HSM server

Once you have configured the HSM server on FortiAuthenticator, you can create a local CA certificate using the HSM server to sign requests. For more information on setting up a certificate authority, see FortiAuthenticator as a Certificate Authority on page 8.

To create a new local CA certificate using HSM:

1. On FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs*, and click *Create New*.



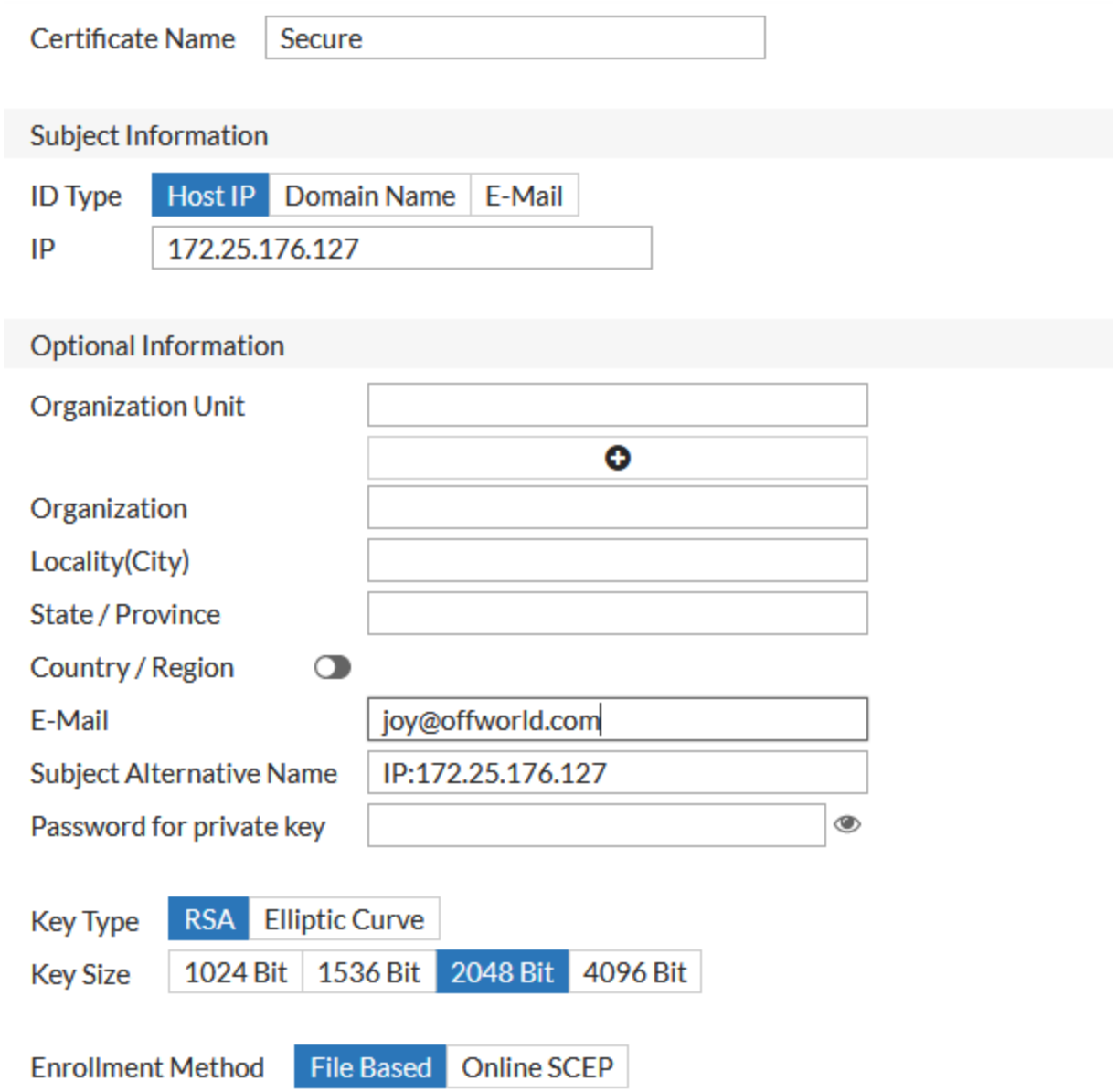
2. Enter a name for the CA certificate, for example *My_CA*.
3. Select *Root CA* as the *Certificate type*.
4. Enable *Use NetHSM*, and choose an HSM server from the dropdown menu.
5. Configure the remaining settings as desired, and click *OK* to save your changes.
   Once your CA certificate has been created, it can be exported and installed on your network. For more information on setting up a certificate authority, see FortiAuthenticator as a Certificate Authority on page 8.

Creating a CSR on the FortiGate

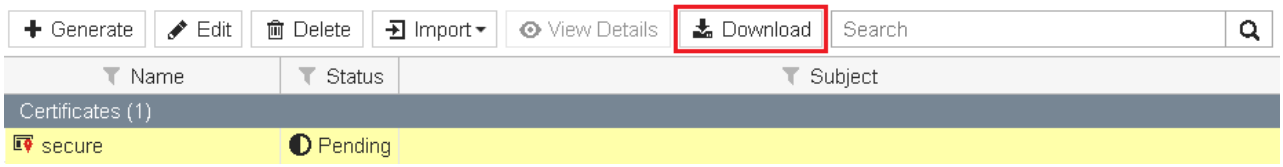
To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.

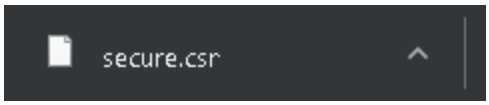
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



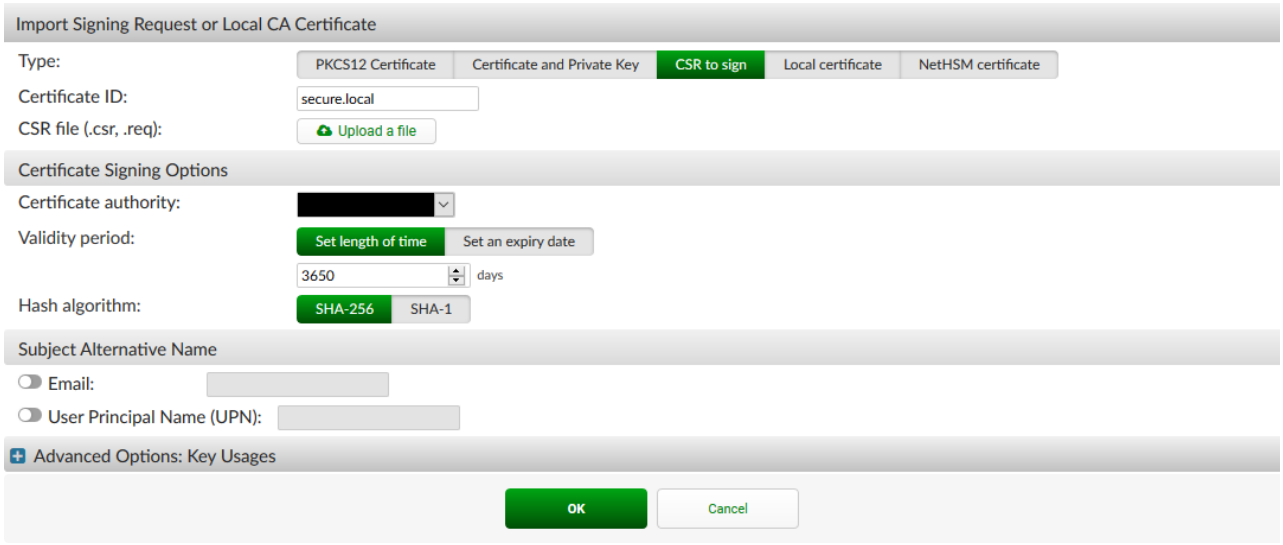
This will save a **.csr** file to your local drive.



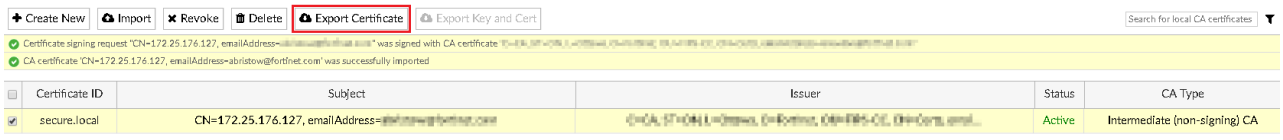
Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

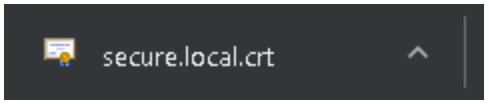
1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file.
2. Select the *Certificate authority* configured with the HSM from the dropdown menu, and set the *Hash algorithm* to *SHA-256*. Click *OK*.



3. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, showing a *Status* of *Active*, and with the *CA Type* of *Intermediate (non-signing) CA*.
4. Highlight the certificate and select *Export Certificate*.



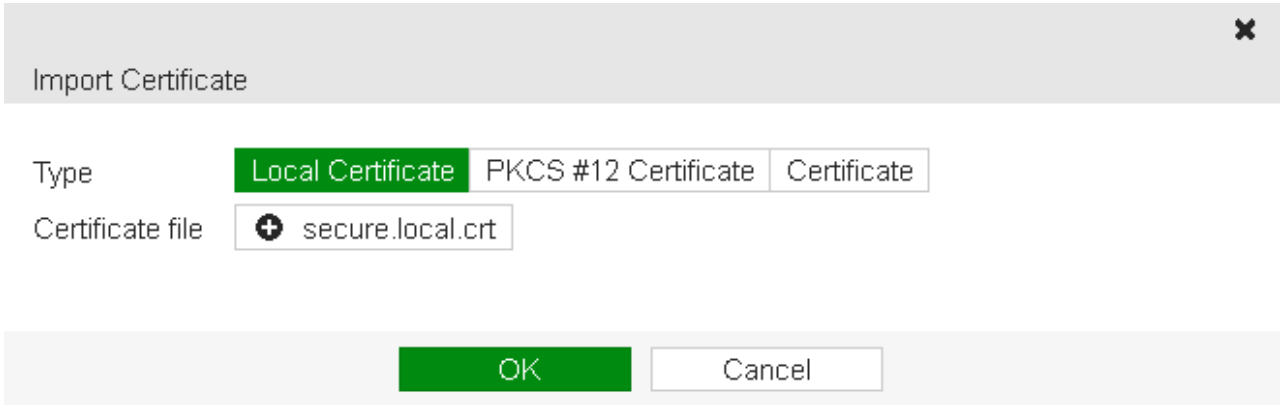
This will save a *.crt* file to your local drive.



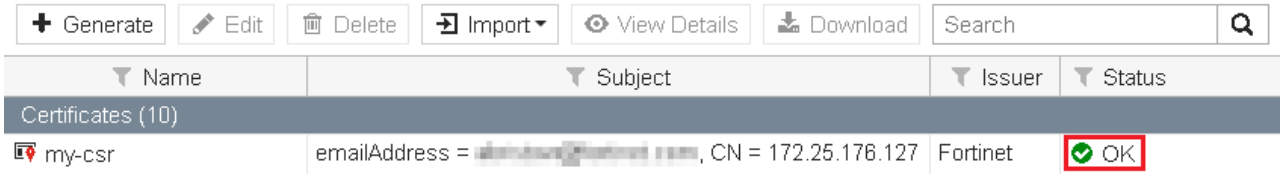
Importing the signed certificate on the FortiGate

To import the signed certificate:

1. Back on the FortiGate, go to *System* > *Certificates* and select *Import* > *Local Certificate*.
   Browse to the *.crt* file, and select *OK*.



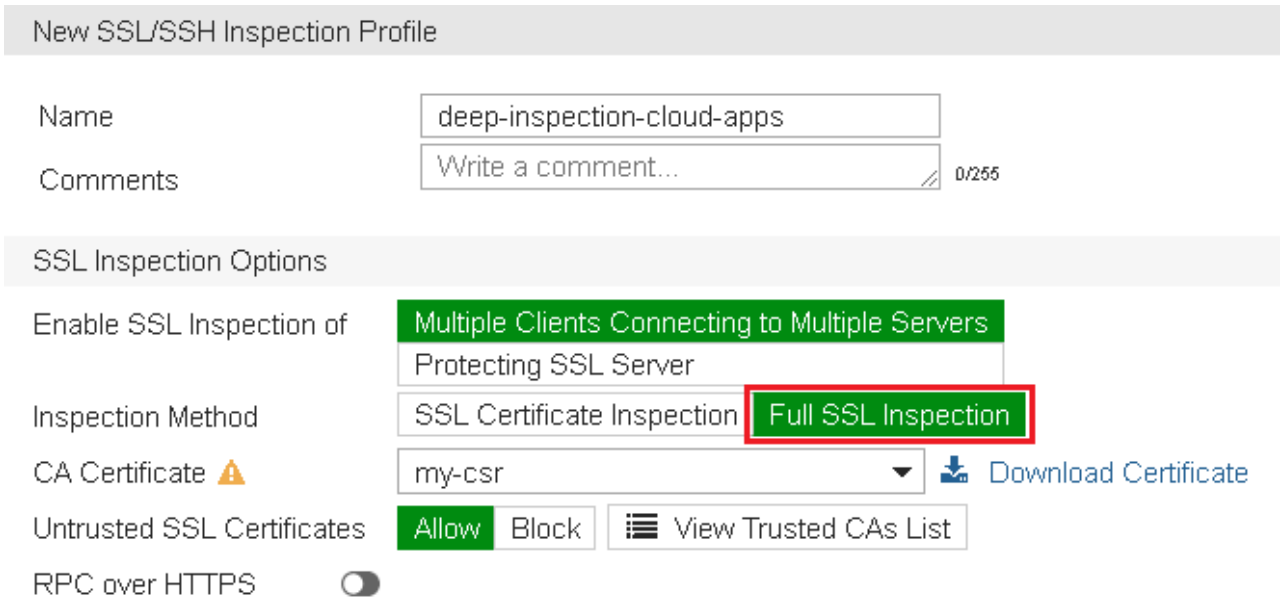
2. You should now see that the certificate has a *Status* of *OK*.



Configuring full SSL inspection

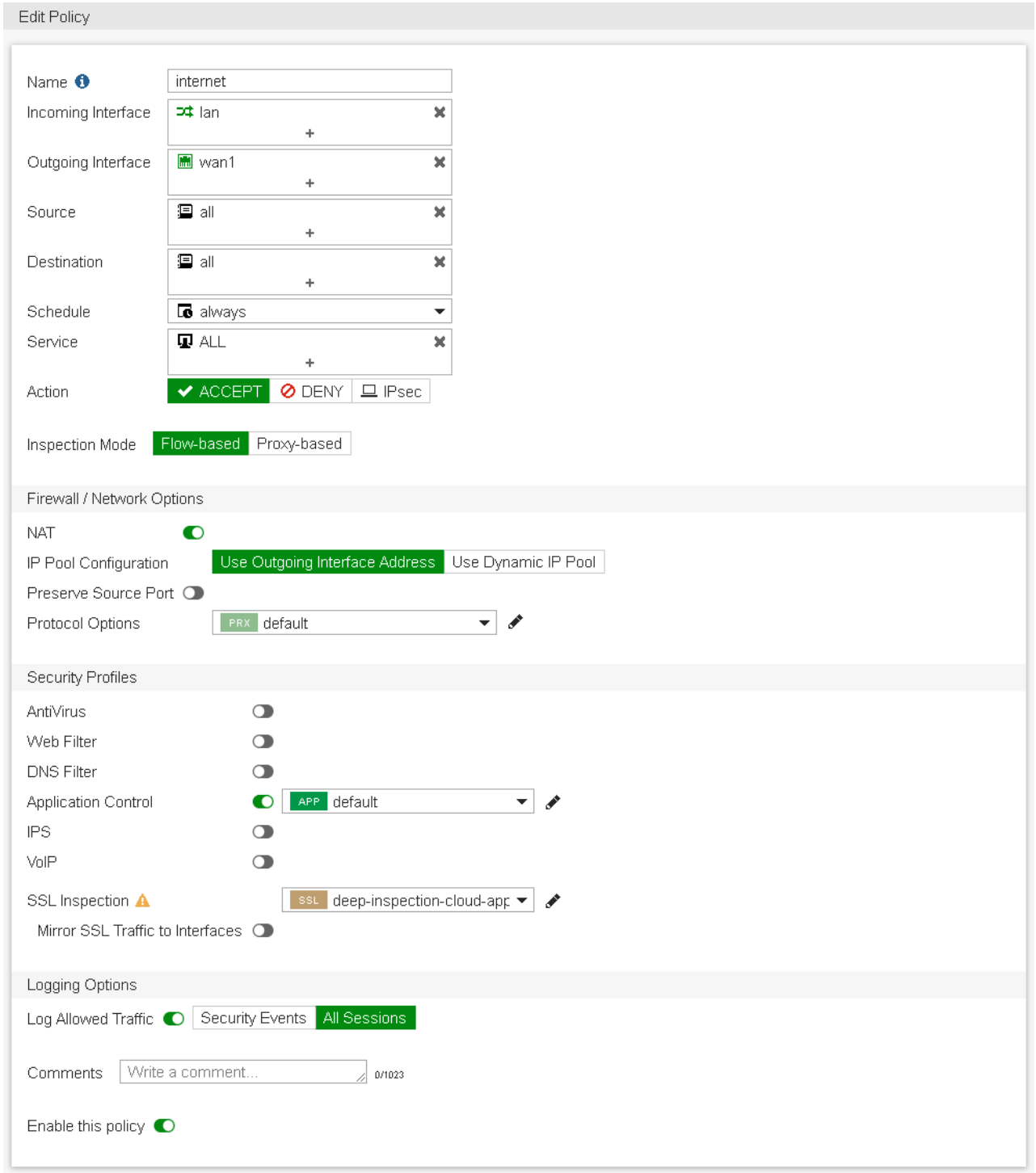
To configure full SSL inspection:

1. On the FortiGate, go to *Security Profiles* > *SSL/SSH Inspection*, and create a new profile.
   Enter a *Name*, select the certificate from the *CA Certificate* dropdown menu, and make sure *Inspection Method* is set to *Full SSL Inspection*.



2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.

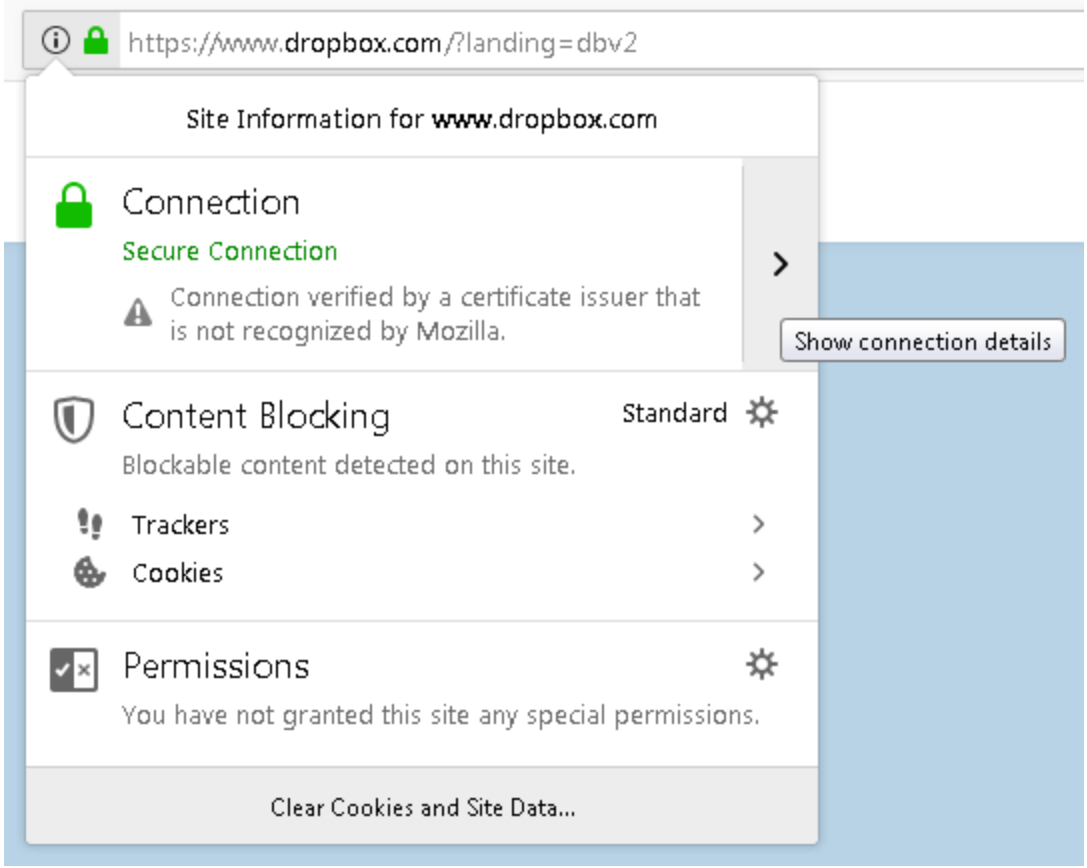
3. Next go to *Policy & Objects* > *IPv4 Policy* and edit the policy that allows Internet access.



4. Under *Security Profiles*, enable *SSL/SSH Inspection* and select the custom profile created earlier.
5. Enable *Application Control* and set it to *default*.

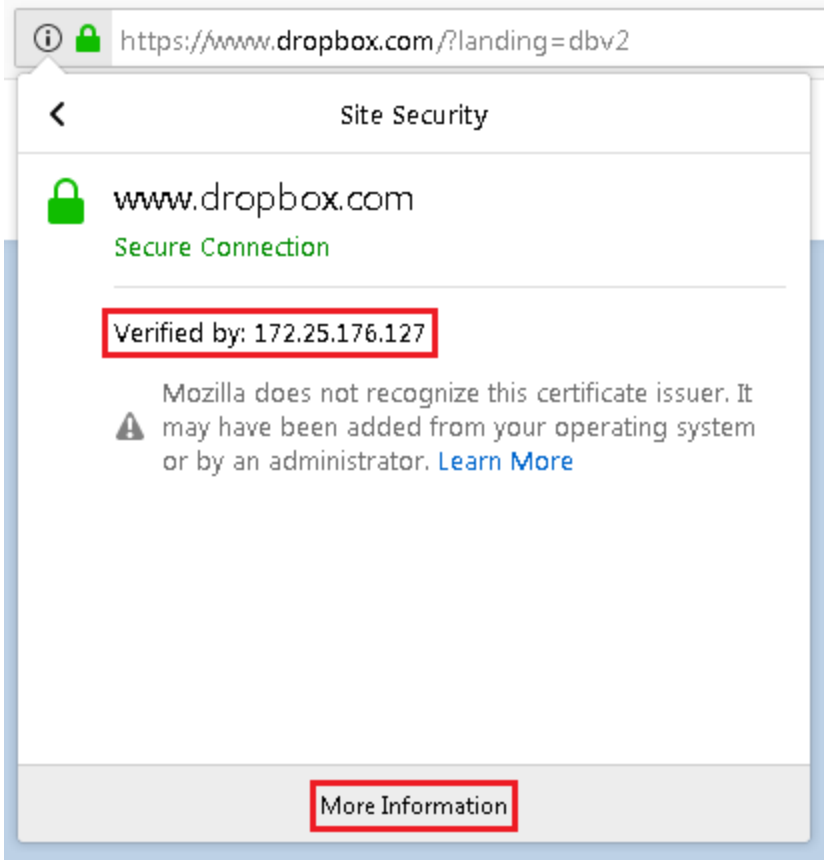
Results

1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, `https://www.dropbox.com`).
   Click on the lock icon next to the address bar, and click *Show connection details*.



2. You should now see that the certificate from the FortiGate has signed and verified access to the site. As a result, no certificate errors will appear.

Optionally select *More Information*.

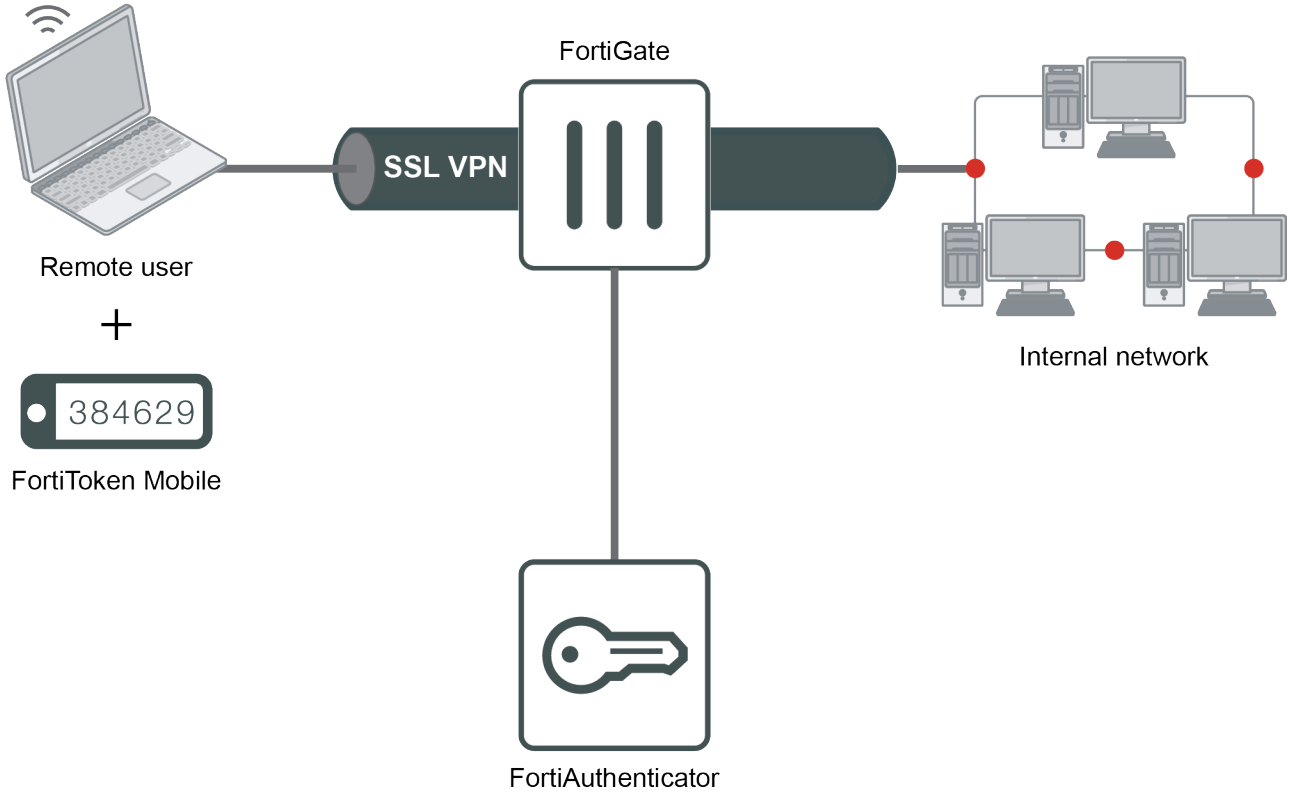


FortiToken and FortiToken Mobile

This section describes various authentication scenarios involving FortiToken, a disconnected one-time password (OTP) generator that's either a physical device or a mobile token. Time-based token passcodes require that the FortiAuthenticator clock is accurate. If possible, configure the system time to be synchronized with a network time protocol (NTP) server.

To perform token-based authentication, the user must enter the token passcode. If the user's username and password are also required, this is called two-factor authentication.

FortiToken Mobile Push for SSL VPN



In this recipe, you set up FortiAuthenticator to function as a RADIUS server to authenticate SSL VPN users using FortiToken Mobile Push two-factor authentication. With Push notifications enabled, the user can easily accept or deny the authentication request.

For this configuration, you:

- Create a user on the FortiAuthenticator.
- Assign a FortiToken Mobile license to the user.
- Create the RADIUS client (FortiGate) on the FortiAuthenticator, and enable FortiToken Mobile Push notifications.

- Connect the FortiGate to the RADIUS server (FortiAuthenticator).
- Create an SSL VPN on the FortiGate, allowing internal access for remote users.

The following names and IP addresses are used:

- Username: gthreepwood
- User group: RemoteFTMGroup
- RADIUS server: OfficeRADIUS
- RADIUS client: OfficeServer
- SSL VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

For the purposes of this recipe, a FortiToken Mobile free trial token is used. This recipe also assumes that the user has already installed the FortiToken Mobile application on their smartphone. You can install the application for Android and iOS. For details, see:

- FortiToken Mobile for Android
- FortiToken Mobile for iOS

Adding a FortiToken to the FortiAuthenticator

Before push notifications can be enabled, a *Public IP/FQDN for FortiToken Mobile* must be configured in *System* > *Administration* > *System Access*.

If the FortiAuthenticator is behind a firewall, the public IP/FQDN will be an IP/port forwarding rule directed to one of the FortiAuthenticator interfaces.

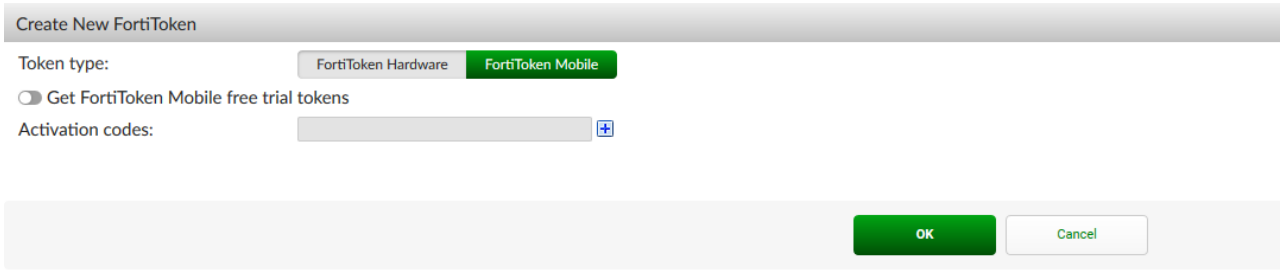
The interface that receives the approve/deny FTM push responses must have the *FortiToken Mobile API* service enabled.

If FortiAuthenticator is not accessible to the Internet, you must create a VIP and policy on FortiGate in order for mobile push to work. The VIP must point from an external port to FortiAuthenticator at port 443.

Once configured, you can add your FortiToken.

To add a FortiToken:

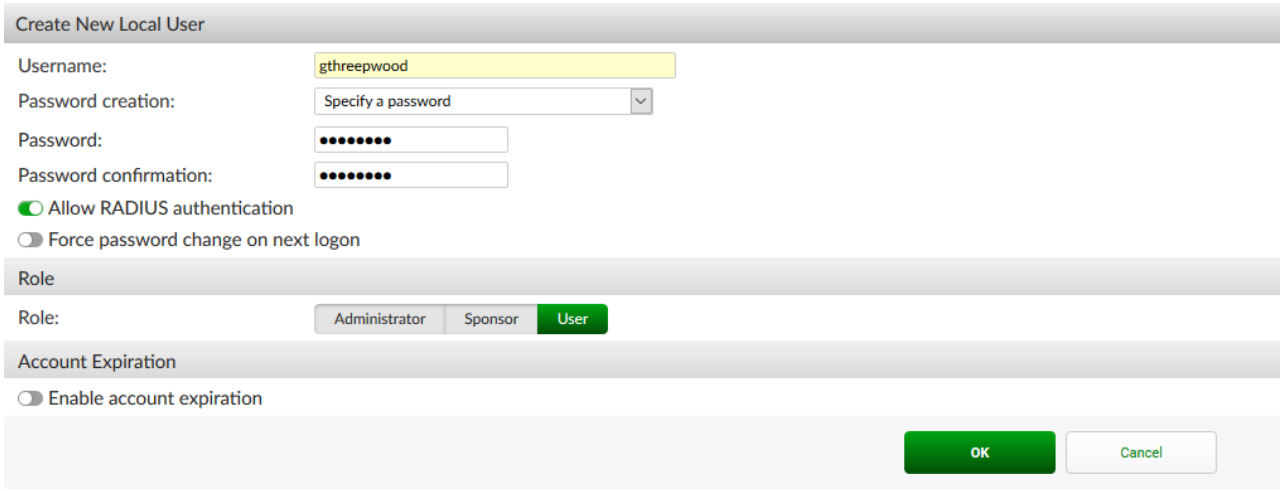
1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *FortiTokens*, and select *Create New*.
2. Set *Token type* to *FortiToken Mobile*, and enter the FortiToken *Activation codes* in the field provided.



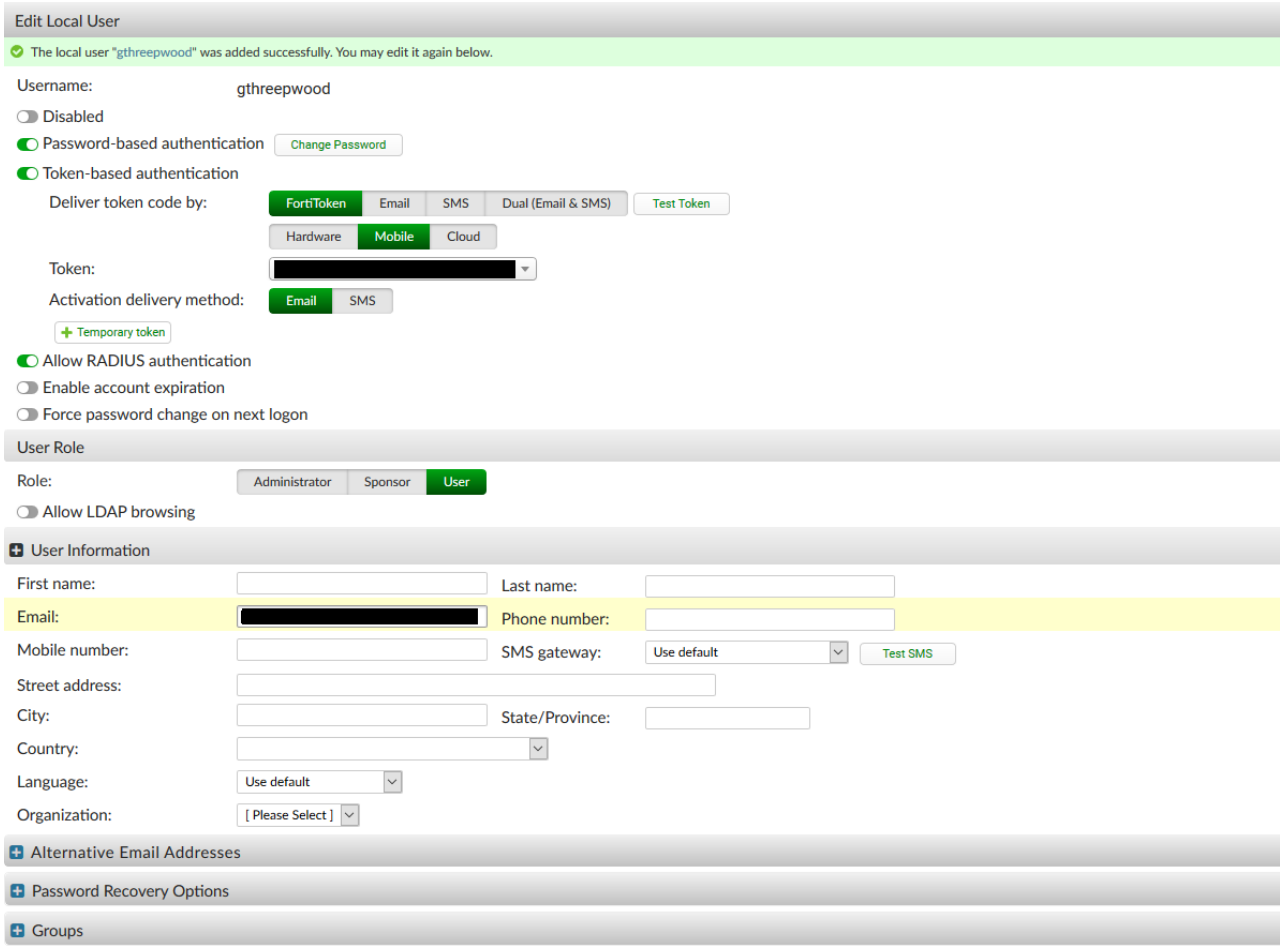
Adding the user to the FortiAuthenticator

To add a user to FortiAuthenticator:

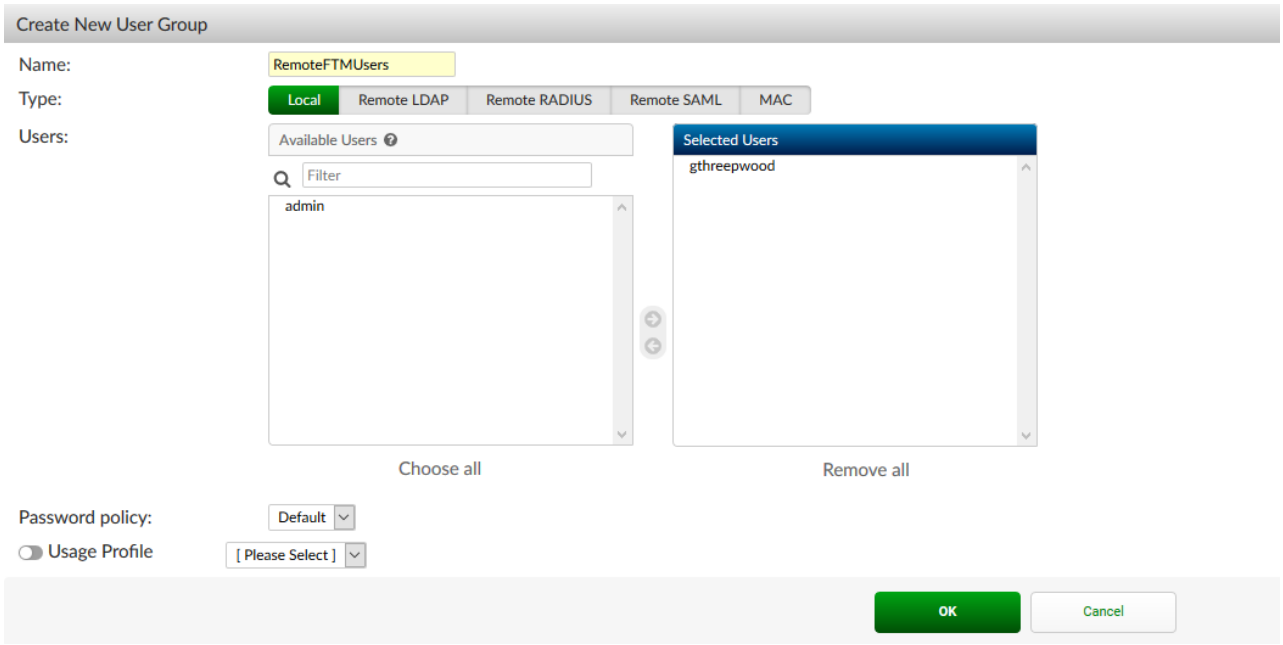
1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users*, and select *Create New*.
   Enter a *Username* (`gthreepwood`) and enter and confirm the user password.
   Enable *Allow RADIUS authentication*, and select *OK* to access additional settings.



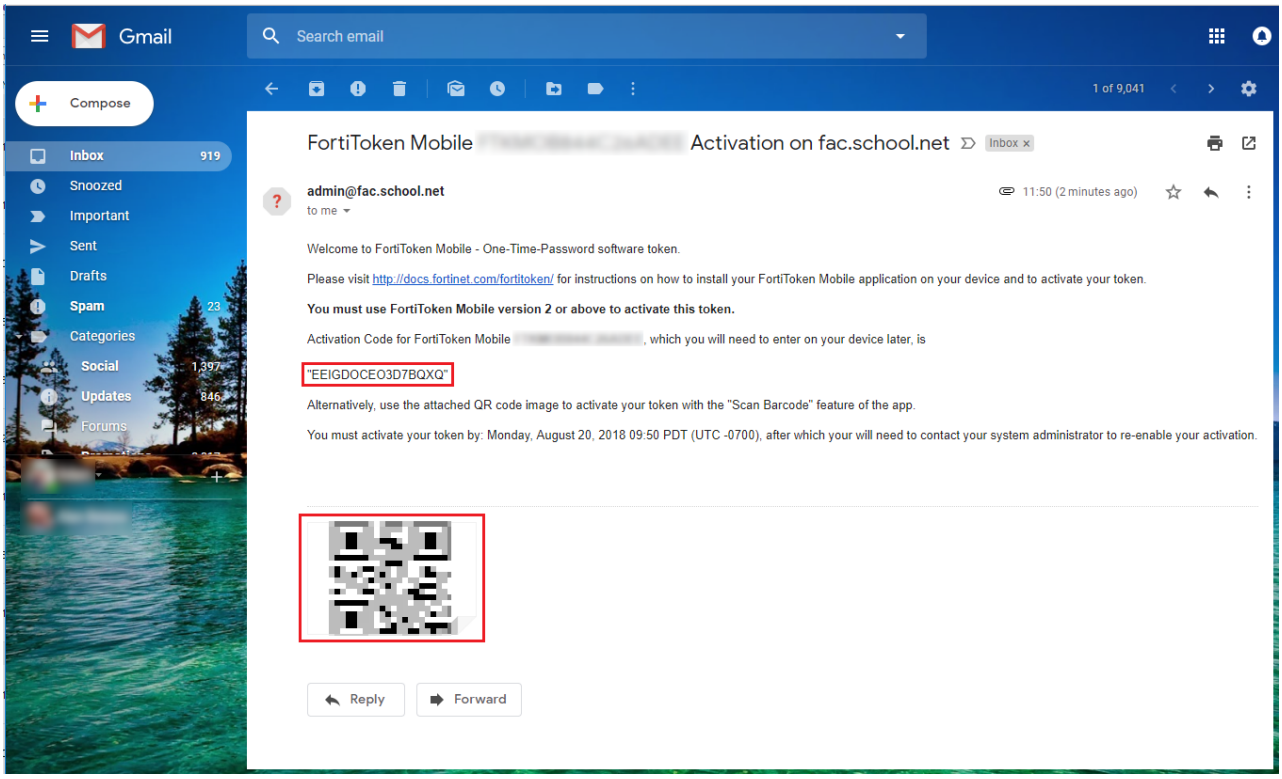
2. Enable *Token-based authentication* and select to deliver the token code by *FortiToken*. Select the FortiToken added earlier from the *FortiToken Mobile* drop-down menu.
   Set *Delivery method* to *Email*. This will automatically open the *User Information* section where you can enter the user email address in the field provided.



3. Next, go to *Authentication* > *User Management* > *User Groups*, and select *Create New*.
Enter a *Name* (`RemoteFTMUsers`) and add gthreepwood to the group by moving the user from *Available users* to *Selected users*.



4. The FortiAuthenticator sends the FortiToken Mobile activation to the user's email address. If the email does not appear in the inbox, check the spam folder.
   The user activates their FortiToken Mobile through the FortiToken Mobile application by either entering the activation code provided or by scanning the QR code attached.



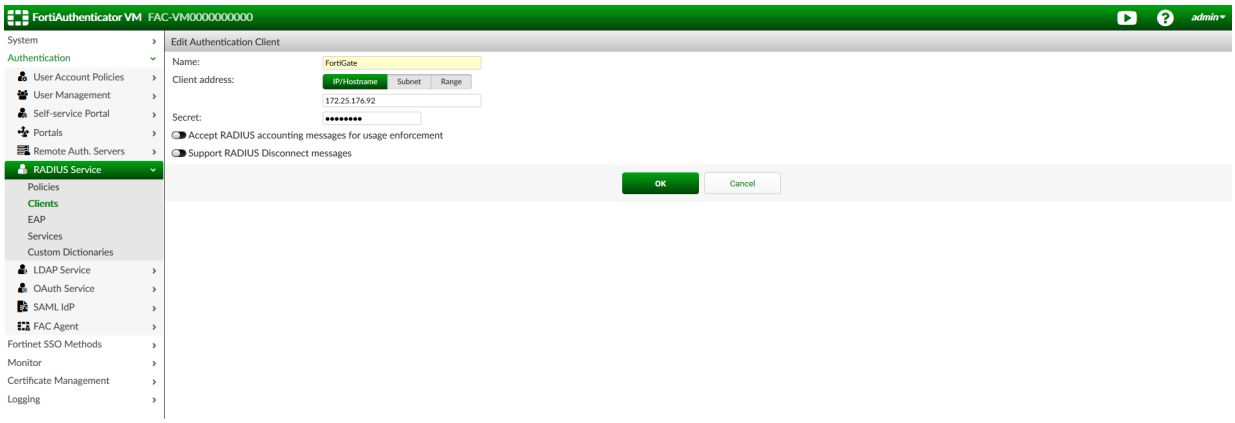
For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client and policy on the FortiAuthenticator

To create the RADIUS client:

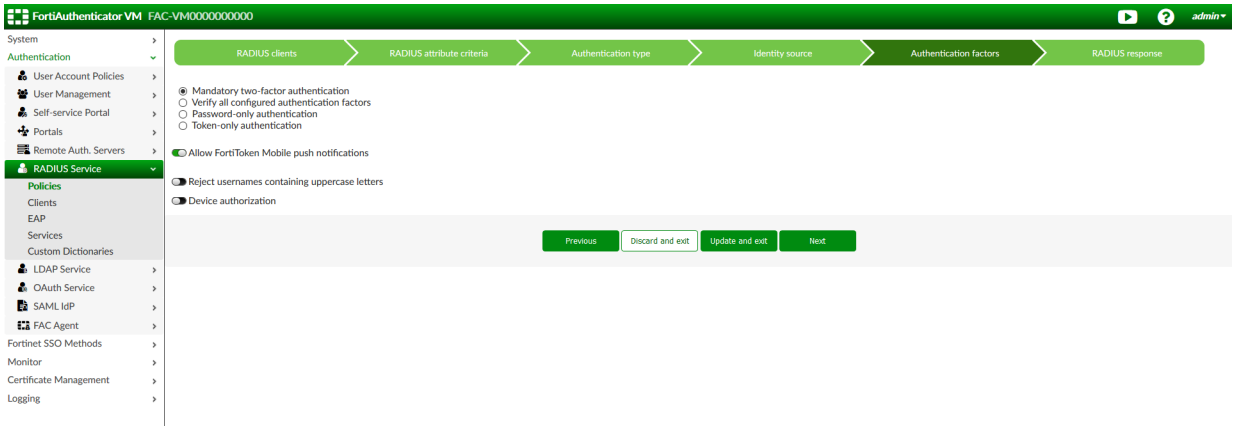
1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New* to add the FortiGate as a RADIUS client.
2. Enter a *Name* (*OfficeServer*), the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.

3. Click *OK*.



To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Optionally, configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type.
5. Choose a username format (in this example: `username@realm`), and select the *Local* realm.
6. Set the authentication method to *Mandatory two-factor authentication*, and enable the *Allow FortiToken Mobile push notifications* option.
7. Click *Save and Exit*.



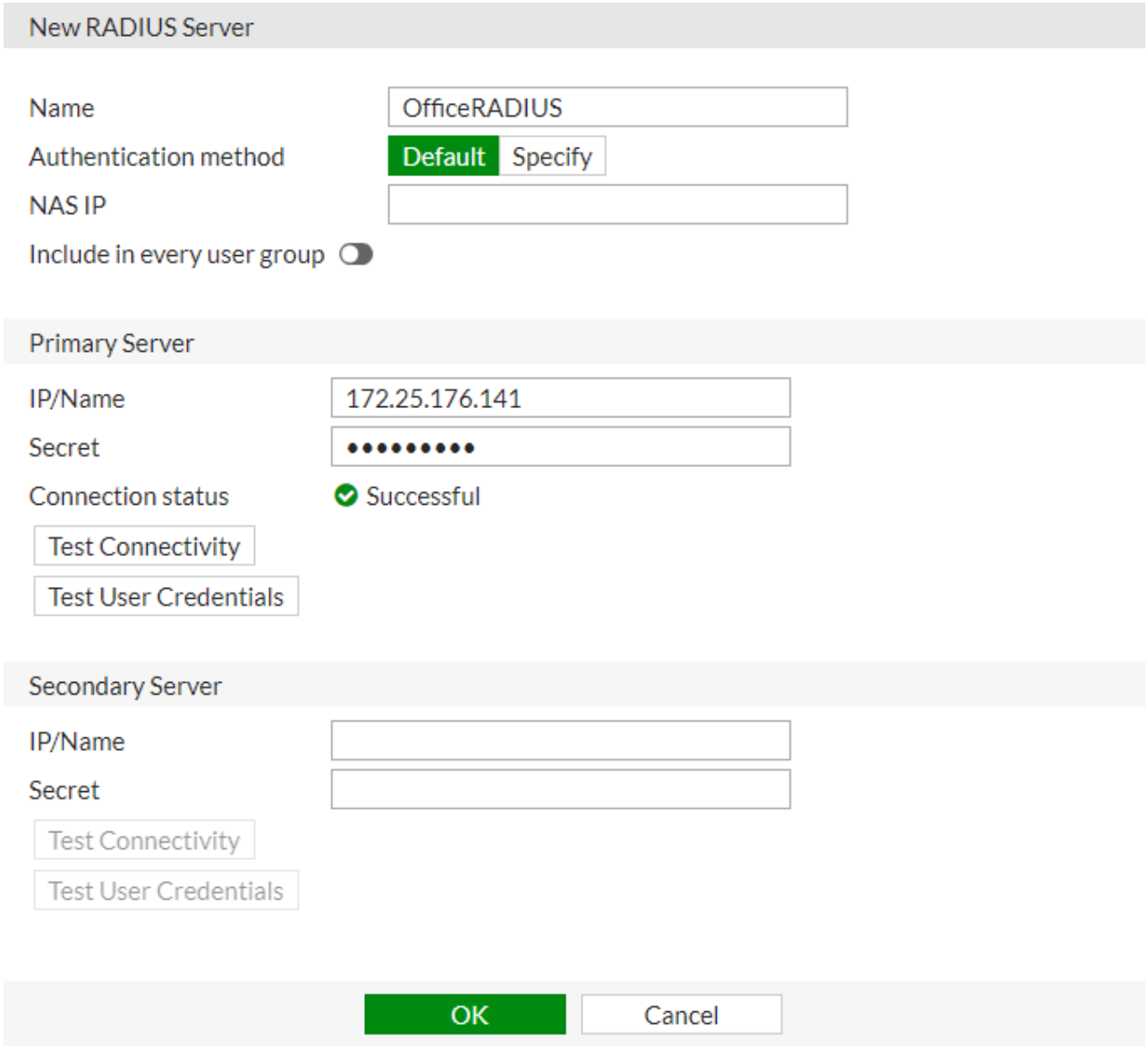
Note the *Username input format*. This is the format that the user must use to enter their username in the web portal, made up of their username and realm. In this example, the full username for gthreepwood is `gthreepwood@local`.

Connecting the FortiGate to the RADIUS server

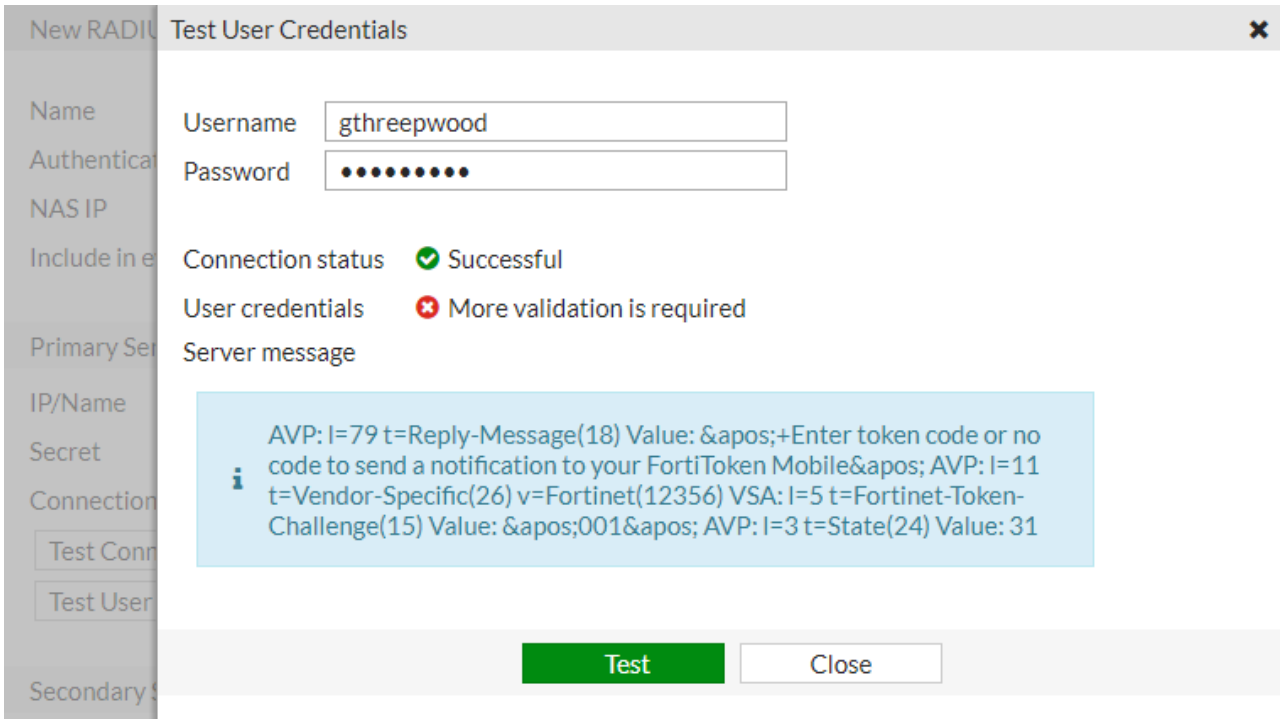
To connect the FortiGate to the RADIUS server:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers*, and select *Create New* to connect to the RADIUS server (FortiAuthenticator).

Enter a *Name* (*OfficeRADIUS*), the IP address of the FortiAuthenticator, and enter the *Secret* created before. Select *Test Connectivity* to be sure you can connect to the RADIUS server. Then select *Test User Credentials* and enter the credentials for *gthreepwood*.

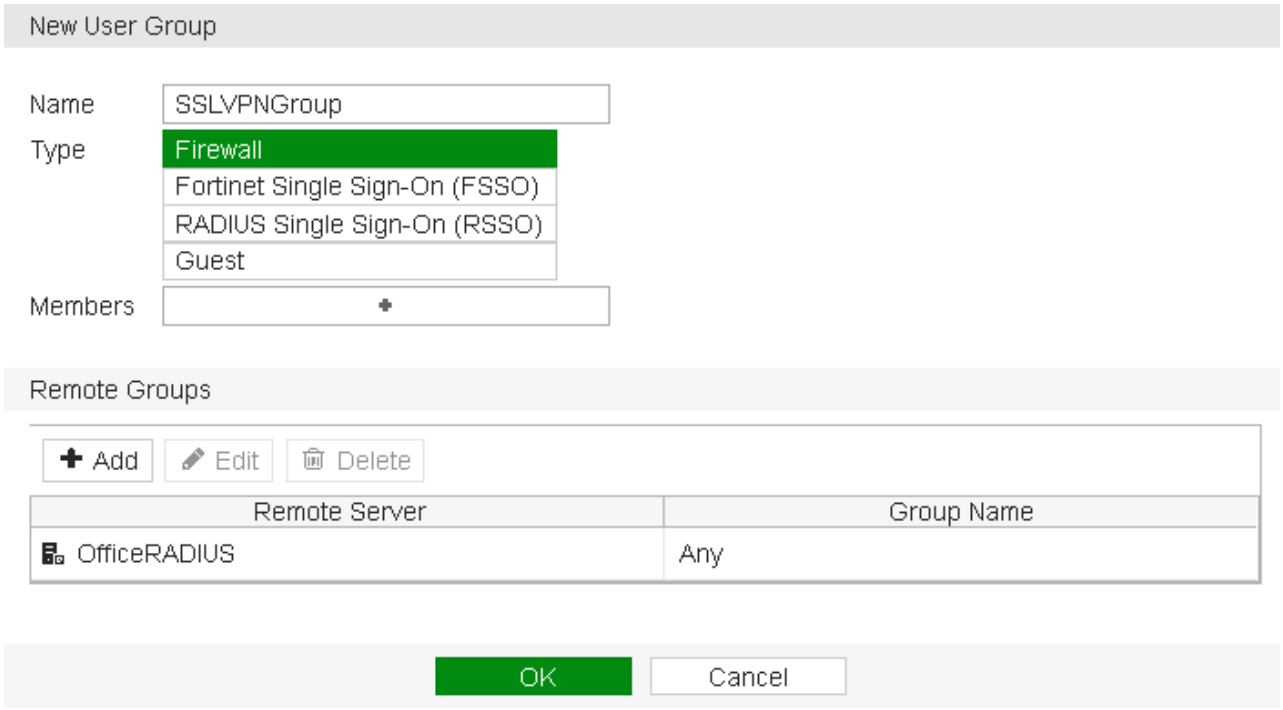


Because the user has been assigned a FortiToken, the test should return stating that *More validation is required*.



The FortiGate can now connect to the FortiAuthenticator as the RADIUS client configured earlier.

2. Then go to *User & Device* > *User Groups*, and select *Create New* to map authenticated remote users to a user group on the FortiGate.
   Enter a *Name* (*SSLVPNGroup*) and select *Add* under *Remote Groups*.
   Select *OfficeRADIUS* under the *Remote Server* drop-down menu, and leave the *Groups* field blank.



3. In the FortiGate CLI, increase the remote authentication timeout to 60 seconds.

```
#config system global
```

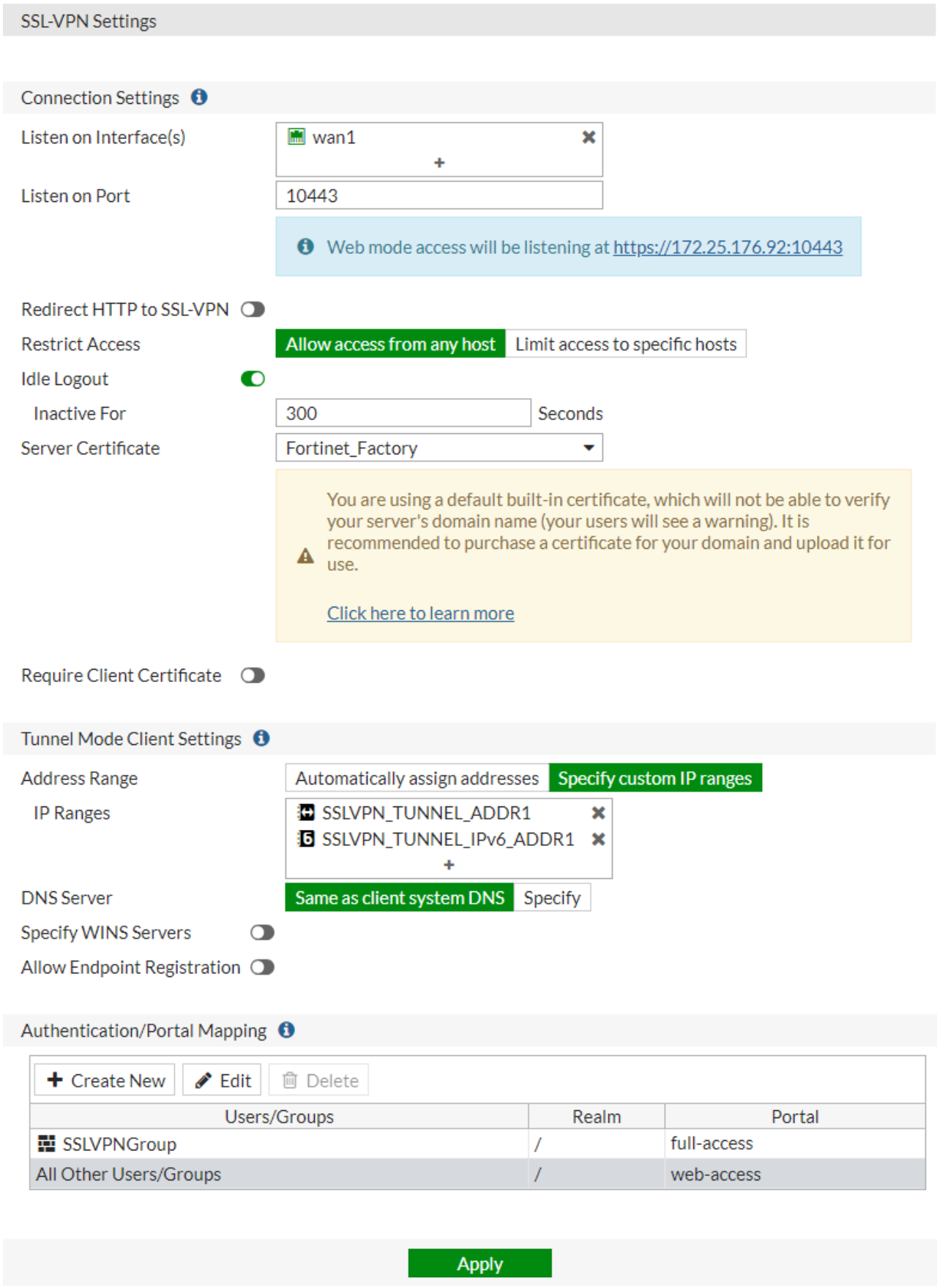
```
    #set remoteauthtimeout 60
#end
```

Configuring the SSL-VPN

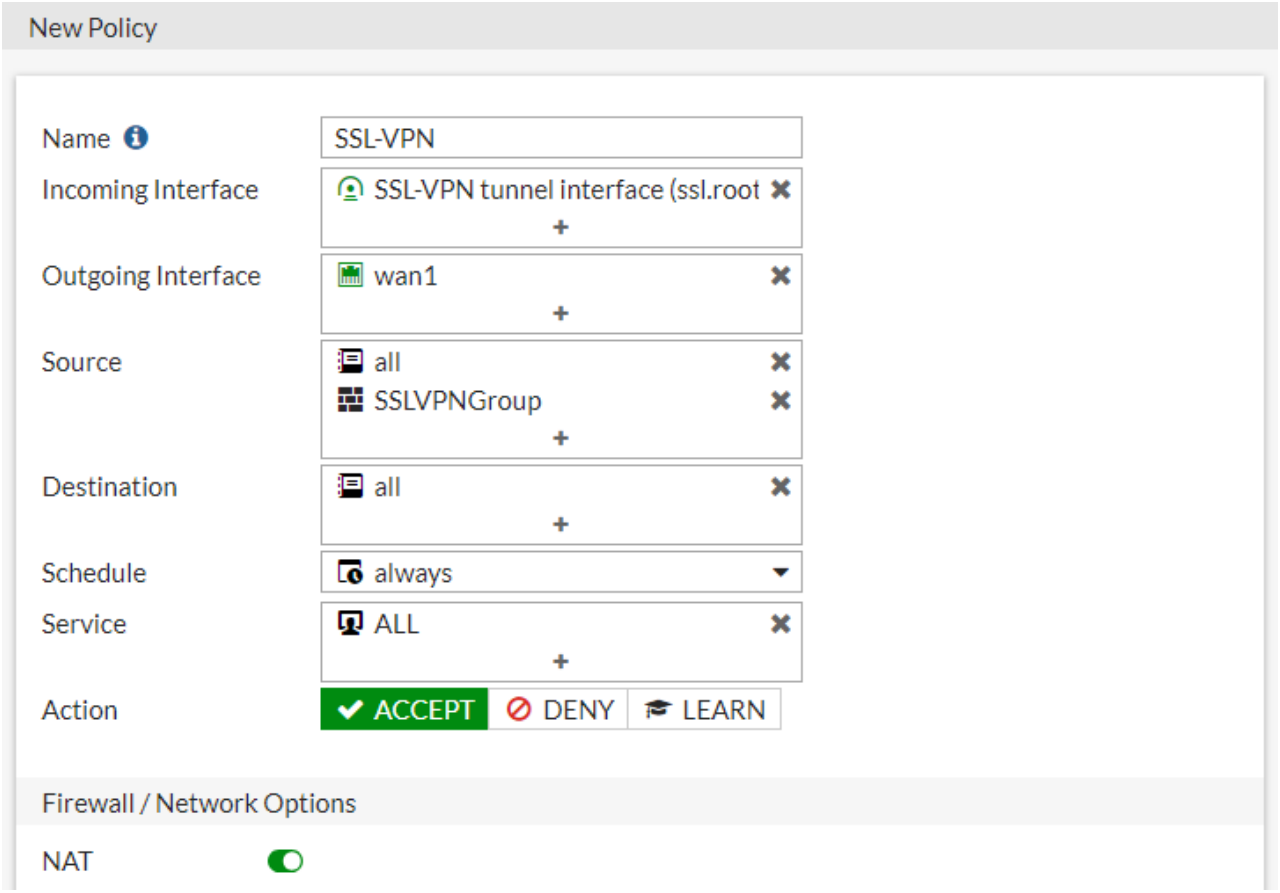
To configure the SSL-VPN:

1. On the FortiGate, go to *VPN* > *SSL-VPN Portals*, and edit the *full-access* portal.
   Toggle *Enable Split Tunneling* so that it is disabled.

2. Go to *VPN* > *SSL-VPN Settings*.
   Under *Connection Settings* set *Listen on Interface(s)* to *wan1* and *Listen on Port* to `10443`.
   Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges*. The *IP Ranges* should be set to *SSLVPN_TUNNEL_ADDR1* and the IPv6 version by default.
   Under *Authentication/Portal Mapping*, select *Create New*.
   Set the *SSLVPNGroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to *web-access* — this will grant all other users access to the web portal *only*.

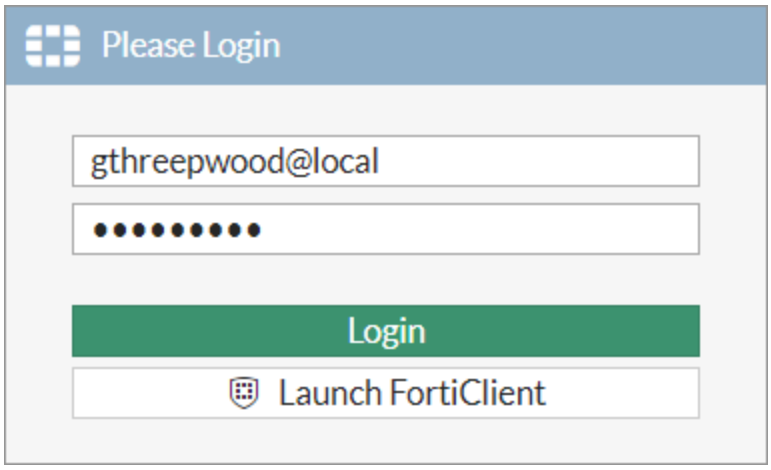

SSL-VPN Settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.92:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
IP Ranges
SSLVPN_TUNNEL_ADDR1
SSLVPN_TUNNEL_IPv6_ADDR1
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
Portal
SSLVPNGroup
/
full-access
All Other Users/Groups
/
web-access
Apply

3. Then go to *Policy & Objects* > *IPv4 Policy* and create a new SSL VPN policy.
   Set *Incoming Interface* to the *SSL-VPN tunnel interface* and set *Outgoing Interface* to the Internet-facing interface (in this case, *wan1*).
   Set *Source* to the *SSLVPNGroup* user group and the *all* address.
   Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and enable *NAT*.

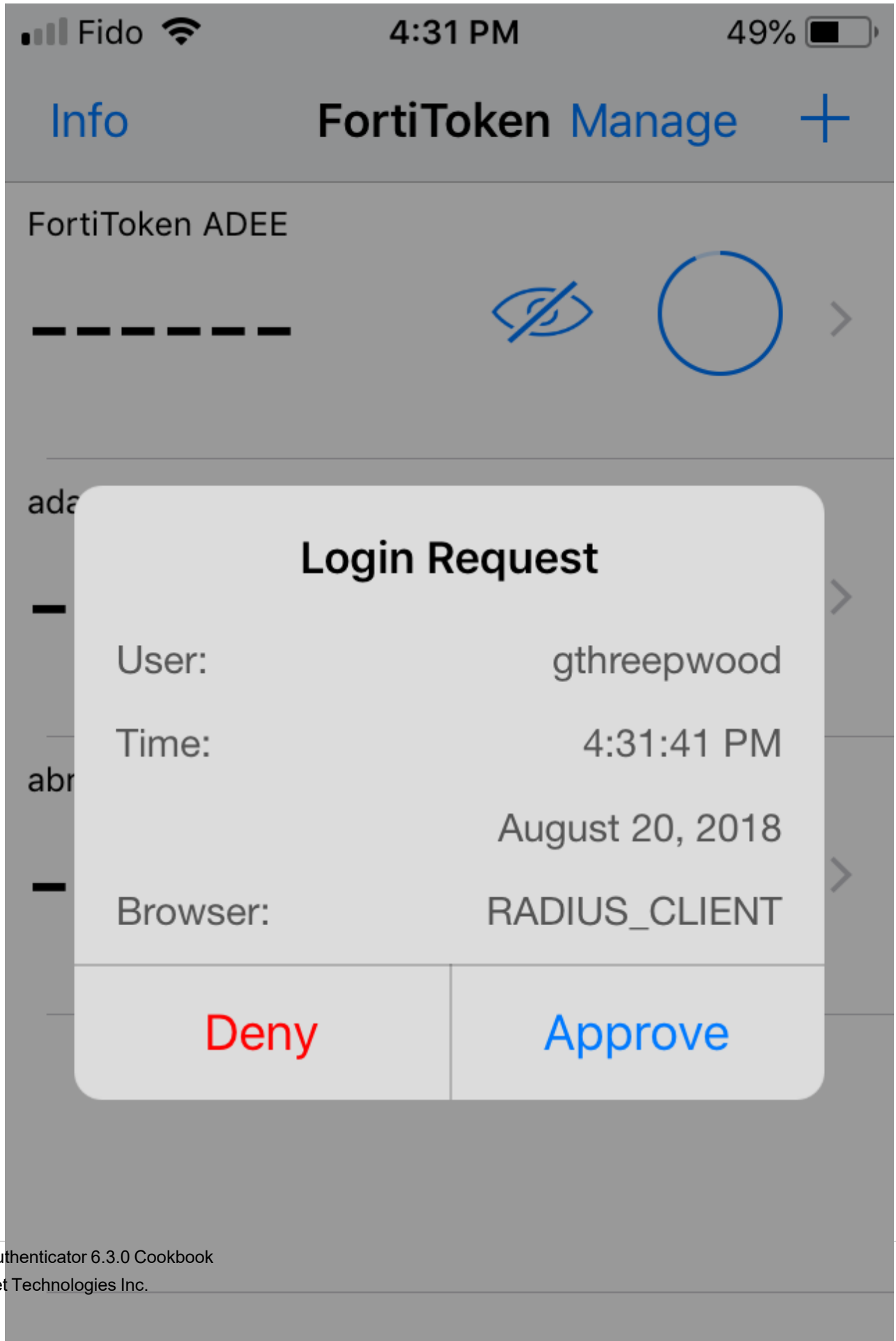


Results

1. From a remote device, open a web browser and navigate to the SSL VPN web portal (*https://<fortigate-ip>:10443*).
2. Enter *gthreepwood's* credentials and select *Login*. Use the correct format (in this case, *username@realm*), as per the client configuration on the FortiAuthenticator.

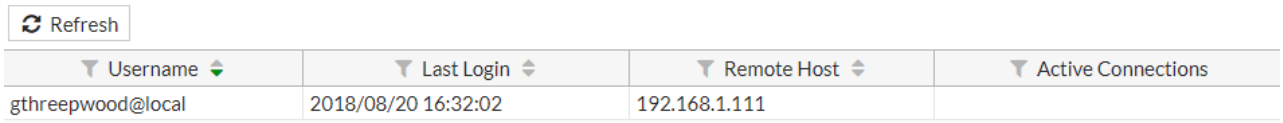


3. The FortiAuthenticator will then push a login request notification through the FortiToken Mobile application. Select *Approve*.


Fido
4:31 PM
49%
Info
FortiToken
Manage
FortiToken ADEE
Login Request
User:
gthreepwood
Time:
4:31:41 PM
August 20, 2018
Browser:
RADIUS_CLIENT
Deny
Approve

Upon approving the authentication, *gthreepwood* is successfully logged into the SSL VPN portal.

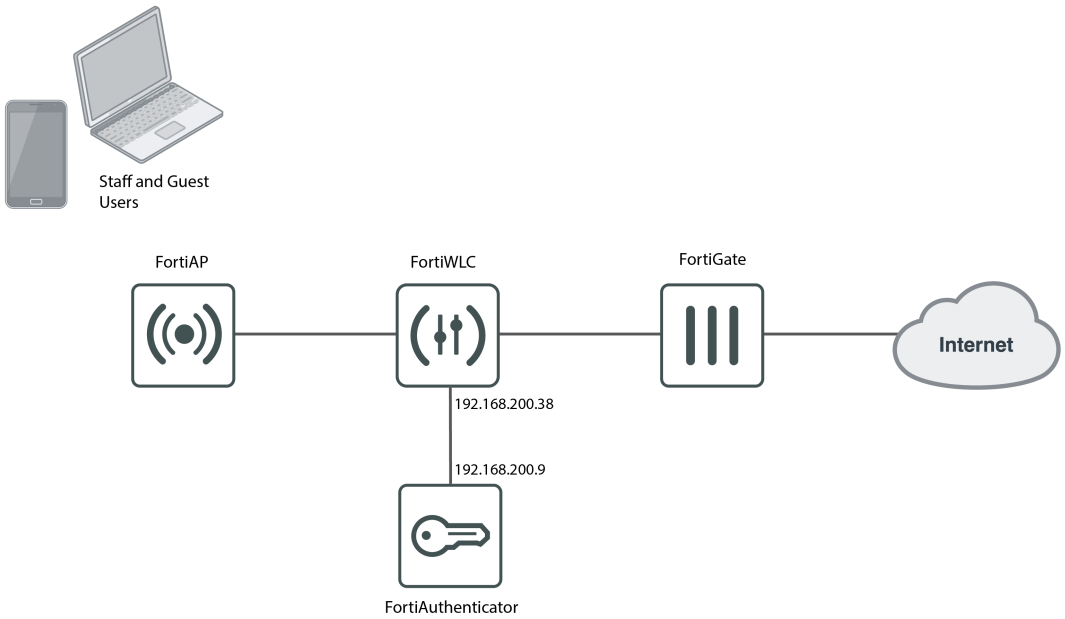
4. On the FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the user's connection.



Guest Portals

This section contains information about creating and using guest portals.

FortiAuthenticator as Guest Portal for FortiWLC

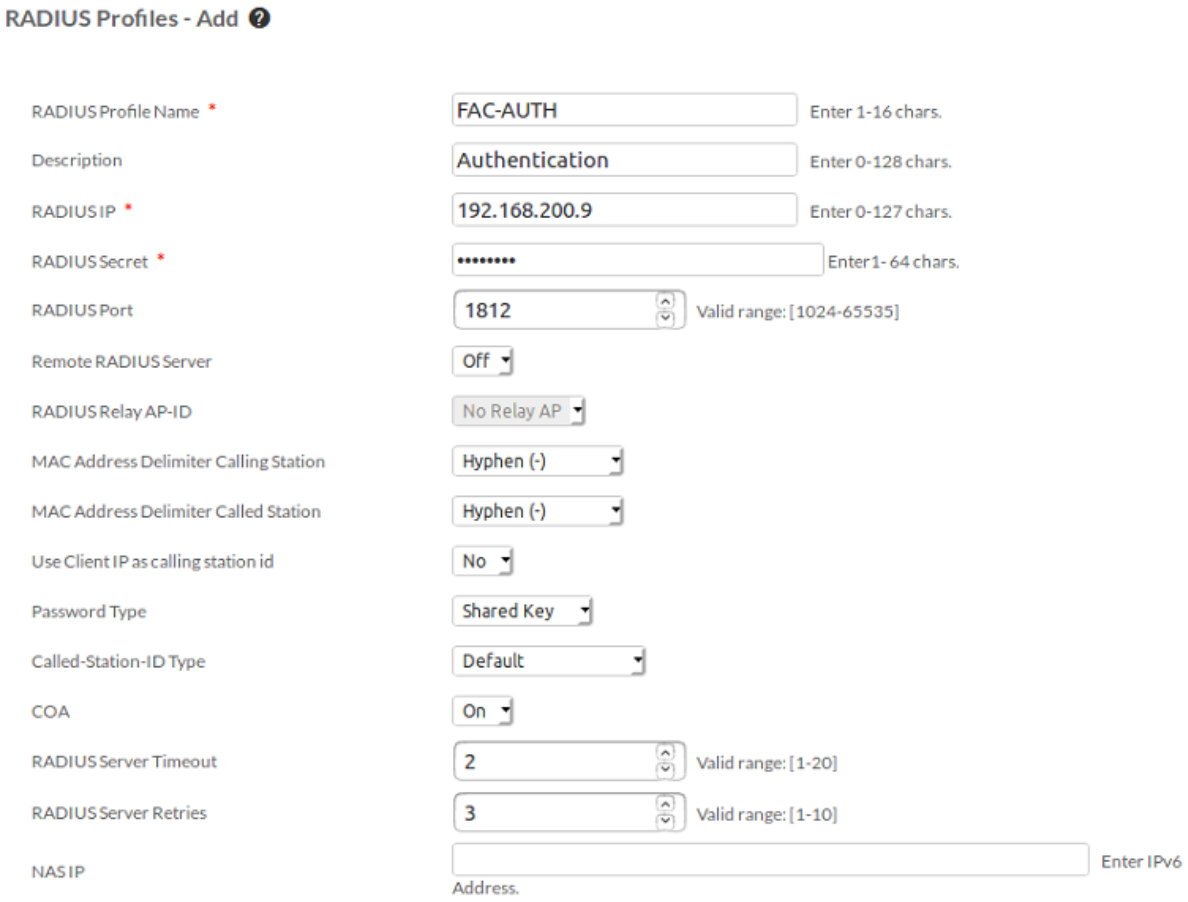


In this recipe we will use FortiAuthenticator as Guest Portal for users getting wireless connection provided by FortiWLC.

Creating the FortiAuthenticator as RADIUS server on the FortiWLC

1. On the FortiWLC, go to *Configuration* > *Security* > *RADIUS* and select *ADD* and create two profiles. One to be used for *Authentication* and one to be used for *Accounting*.
   - *RADIUS Profile name*: Enter a name for the profile. Use a name that will indicate if the profile is used for *Authentication* or *Accounting*.
   - *RADIUS IP*: IP address of the FortiAuthenticator.
   - *RADIUS Secret*: Shared secret between WLC and FortiAuthenticator.

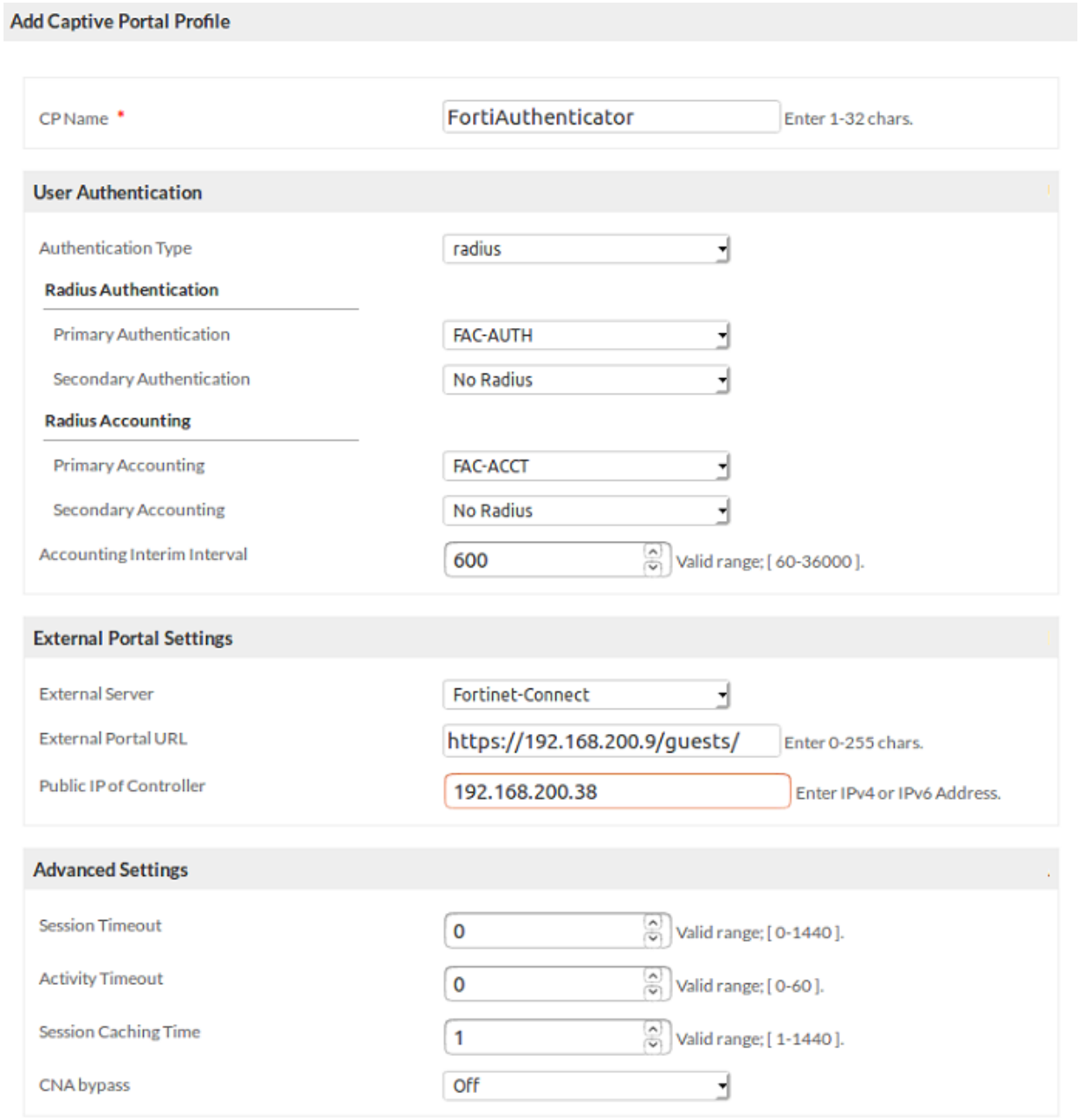
- *RADIUS Port*: Use *1812* for *Authentication* profile and *1813* when creating an *Accounting* profile.



Creating the Captive Portal profile on the FortiWLC

1. On the FortiWLC, go to *Configuration* > *Security* > *Captive Portal*, select the *Captive Portal Profiles* tab, and *ADD* a new profile.
   - *CP Name*: Enter a name for the profile.
   - *Authentication Type*: *RADIUS*
   - *Primary Authentication*:Your Authentication profile.
   - *Primary Accounting*: Your Accounting profile.
   - *External Server*: Fortinet-Connect
   - *External Portal*: https://<fortiauthenticator-ip>/guests

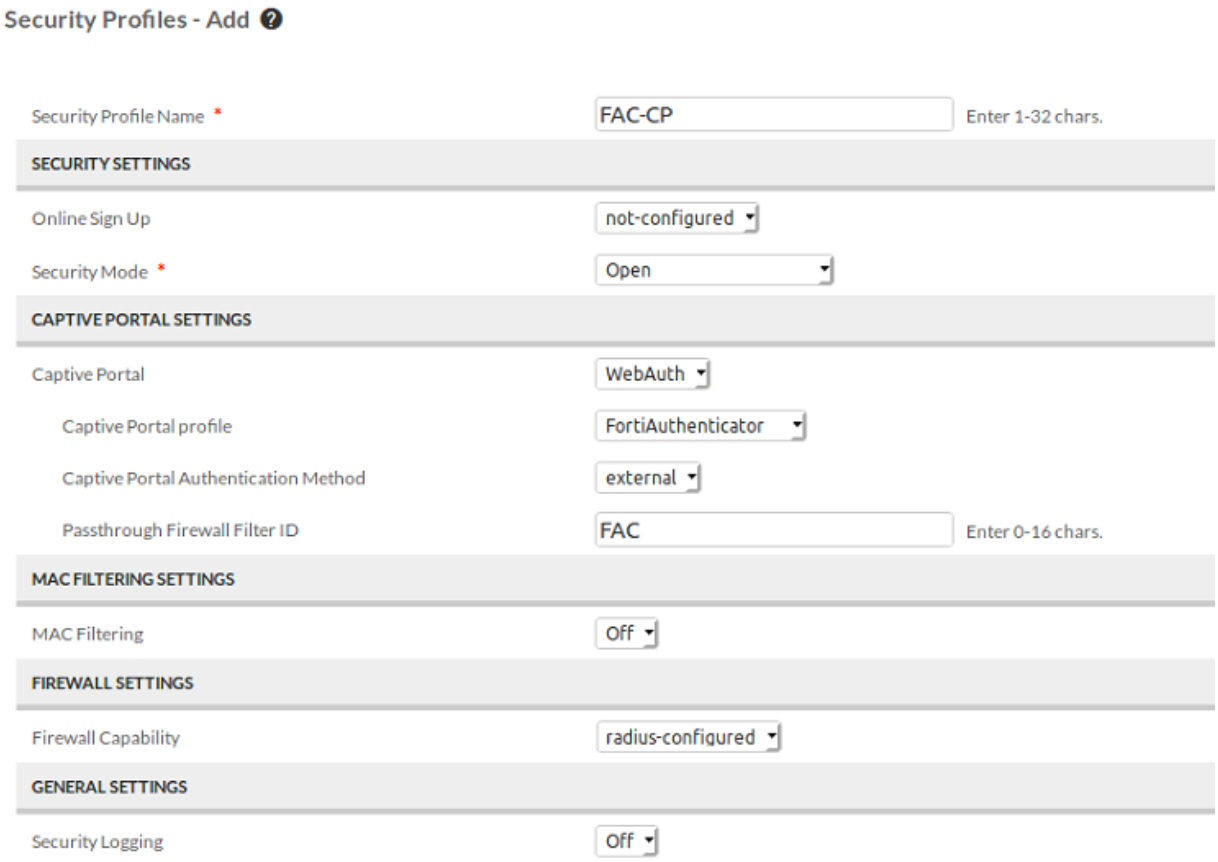
- *Public IP of Controller*: IP address that the FortiAuthenticator can use to communicate with the FortiWLC.



Creating the security profile on the FortiWLC

1. On the FortiWLC, go to *Configuration* > *Security* > *Profile* and *ADD* a new profile.
   - *Profile Name*: Enter a name for the profile.
   - *Security Mode*: *Open*
   - *Captive Portal*: *WebAuth*
   - *Captive Portal Profile*: Select the profile created earlier.
   - *Captive Portal Authentication Method*: *external*

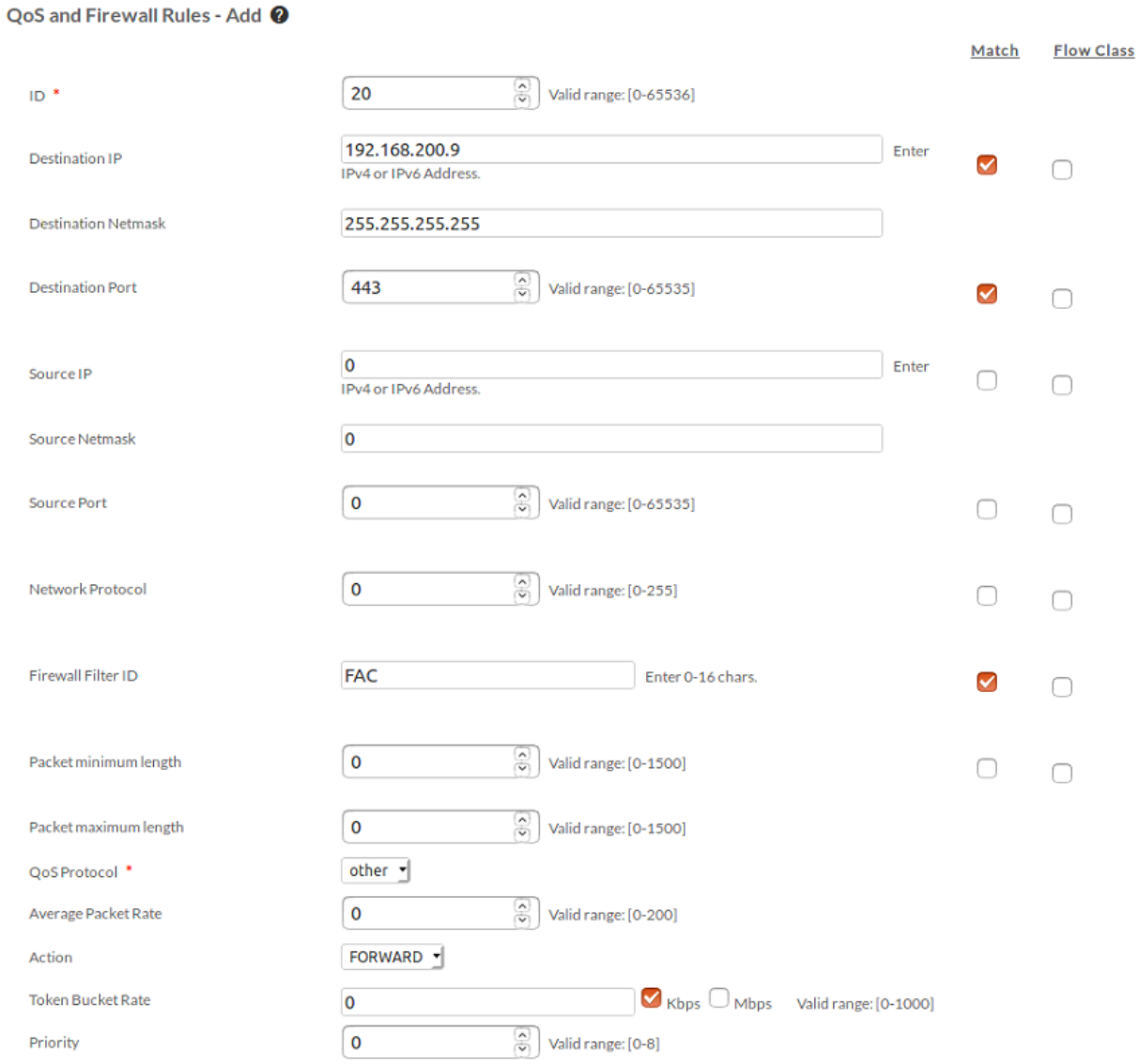
- *Passthrough Firewall Filter ID*: An ID used to allow access to the portal before authentication using QoS rules.



Creating the QoS rule on the FortiWLC

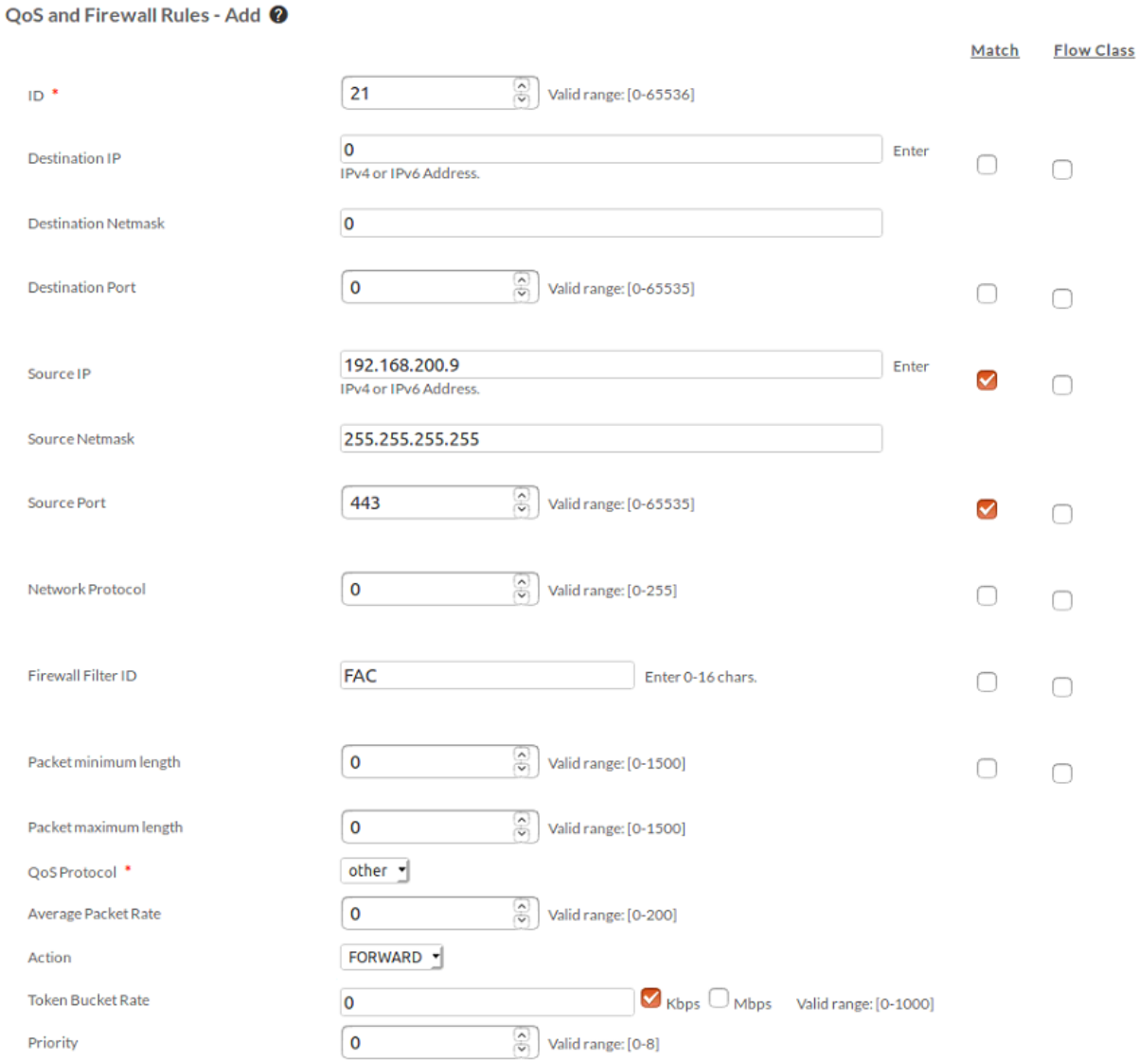
1. On the FortiWLC, go to *Configuration* > *Policies* > *QoS* and select the *QoS and Firewall Rules* tab. Select *ADD* to create two profiles.
   For the first rule, allow the wireless client to access the FortiAuthenticator guest portal.
   - *ID*: Rule number (in the example, *20*).
   - *Destination IP*: IP address of the FortiAuthenticator, and enable *Match*.
   - *Destination Netmask*: *255.255.255.255*
   - *Destination Port*: *443*, and enable *Match*.
   - *Network Protocol*: *6*, and enable *Match*.
   - *Firewall Filter ID*: String from the security profile, and enable *Match*.

- *QoS Protocol*: Other.



2. For the second rule, allow FortiAuthenticator to reach the clients.
   - *ID*: Rule number (in the example, *21*).
   - *Source IP*: IP address of the FortiAuthenticator, and enable *Match*.
   - *Source Netmask*: *255.255.255.255*
   - *Source Port*: *443*, and enable *Match*.
   - *Network Protocol*: *6*, and enable *Match*.
   - *Firewall Filter ID*: Use the *Passthrough Firewall Filter ID* string from the security profile, and enable *Match*.

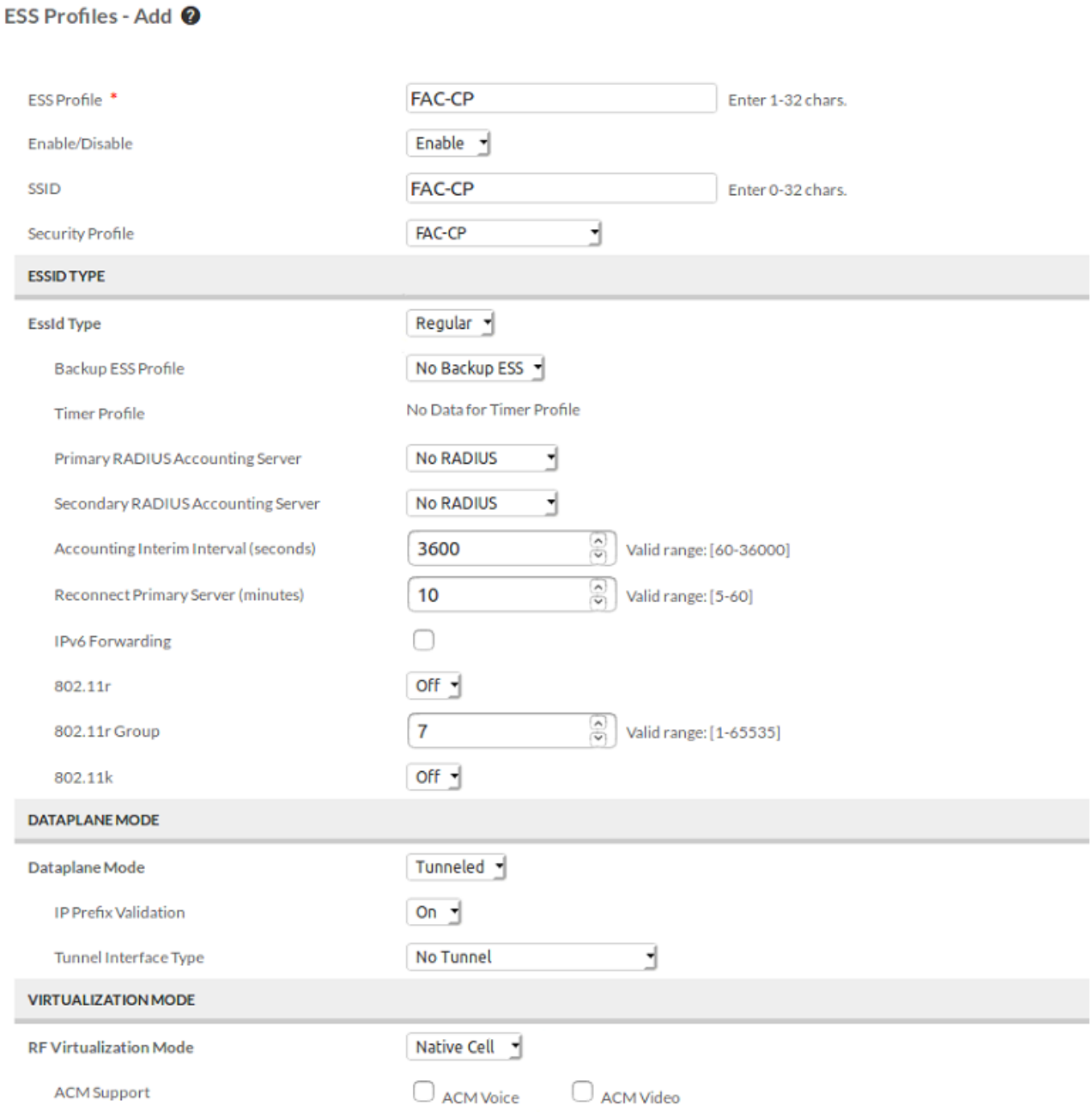
- *QoS Protocol*: Other.



Creating the ESS Profile on the FortiWLC

1. On the FortiWLC, go to *Configuration* > *Wireless* > *ESS* and *ADD* an ESS profile.
   Configure the profile with an appropriate *ESS Profile* and *SSID*. Then select the *Security Profile* that contains the

Captive Portal settings.

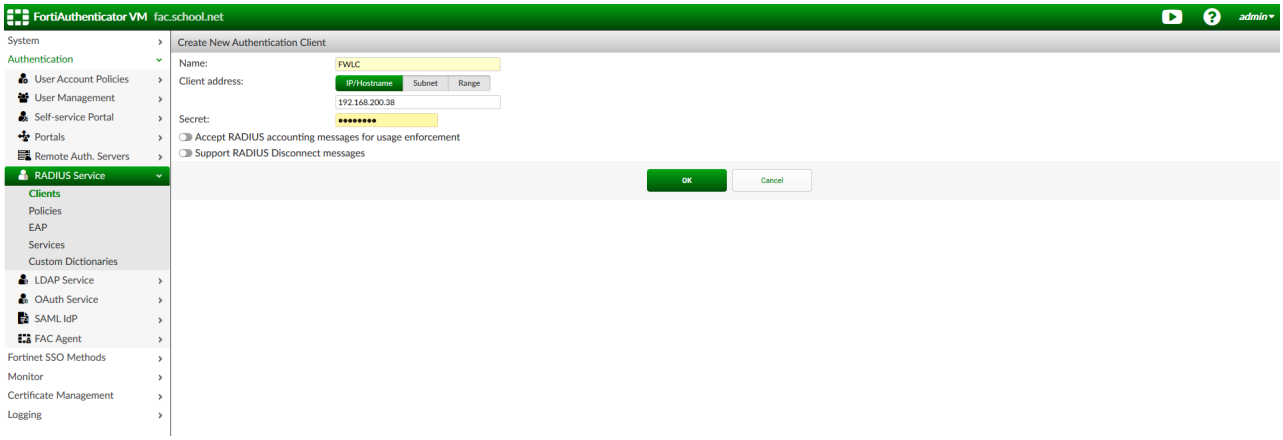


Creating FortiWLC as RADIUS client on the FortiAuthenticator

To create a RADIUS client:

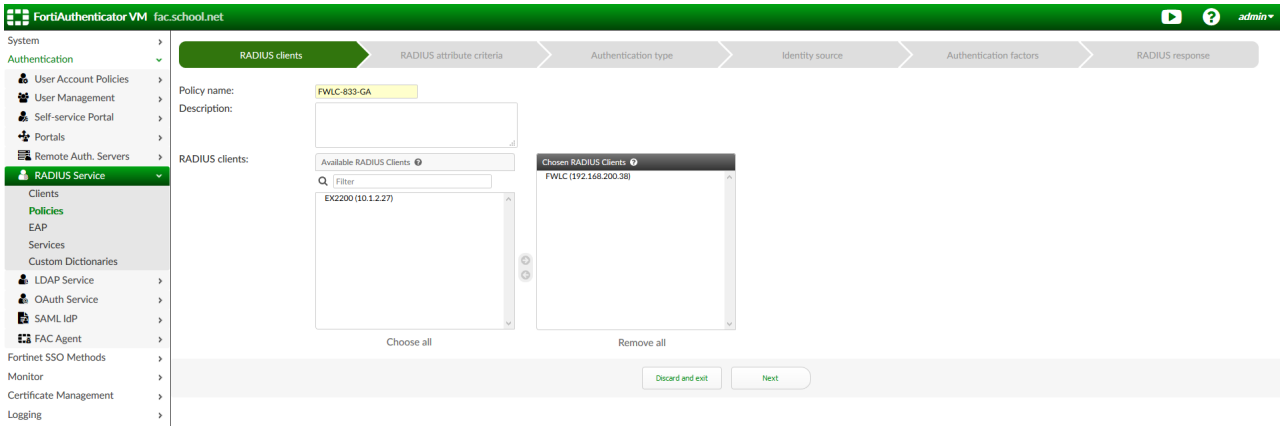
1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients* and create a new client.
   Set *Client address* to *IP/Hostname* and enter the IP address the FortiWLC will send its RADIUS requests from.

Set the same *Secret* that was entered during the RADIUS configuration on the FortiWLC.



To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and create a new policy.



2. In *RADIUS clients*, select the FWLC client previously created.
3. In *RADIUS attribute criteria*, click *Next*. No RADIUS attribute criteria need to be specified in this configuration.
4. In *Authentication type*, select *Password/OTP authentication*. If EAP is being used for wireless authentication, enable *Accept EAP*, along with the desired EAP types.
5. In *Identity source*, select the realm for which user authentication is needed.
6. In *Authentication factors*, select *Verify all configured authentication factors*.
7. Review the *RADIUS response*, and save the policy.

Creating the portal and access point on FortiAuthenticator

To create a portal:

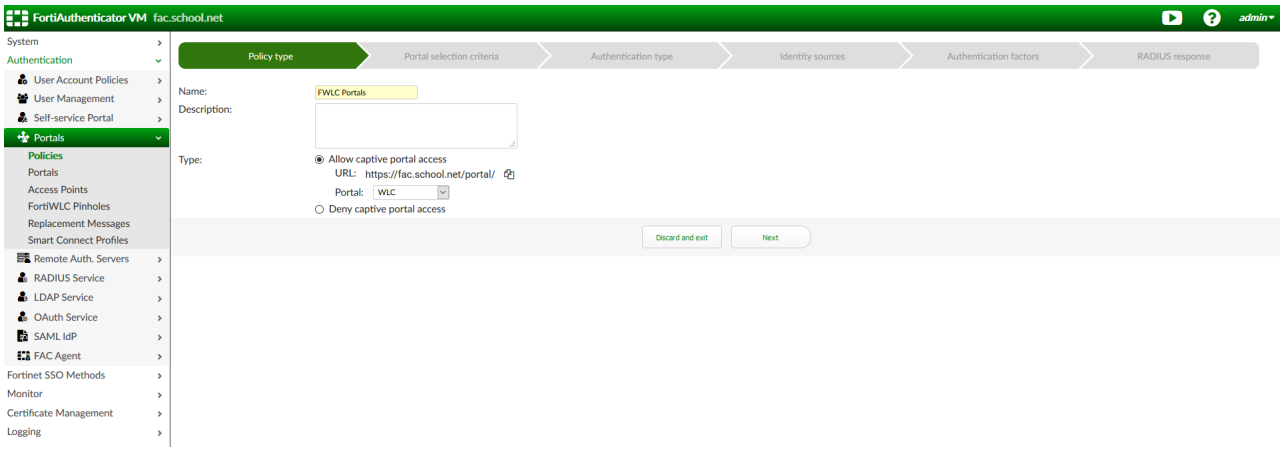
1. On the FortiAuthenticator, go to *Authentication* > *Portals* > *Portals*, and create a new portal.
2. Enter a name for the portal, and click *OK*.

To create an access point:

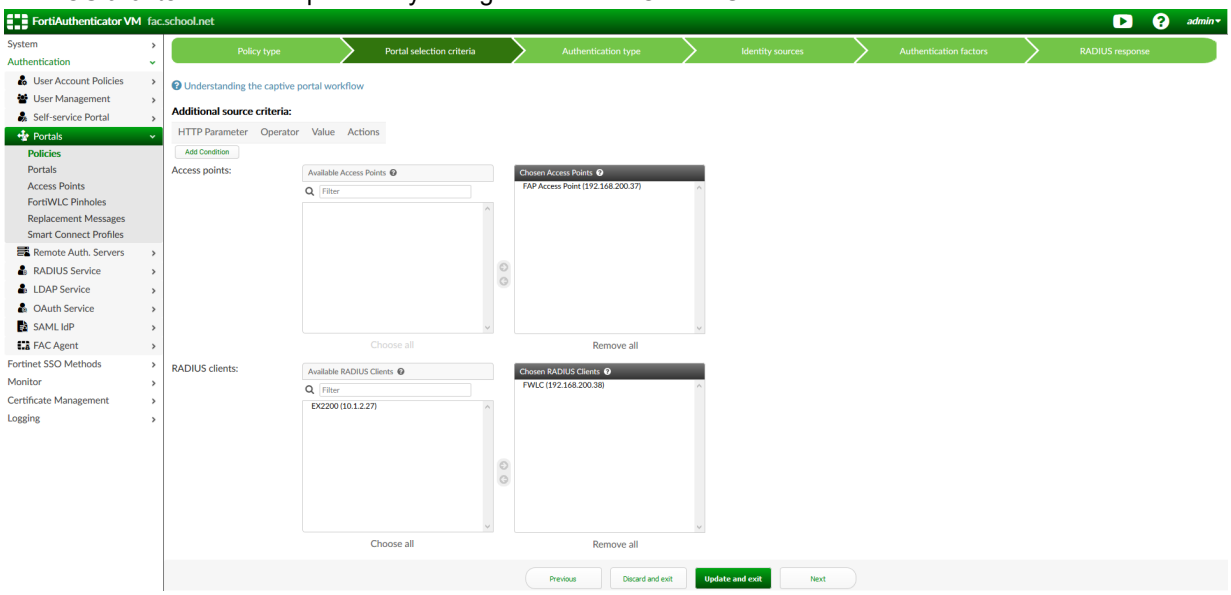
1. On FortiAuthenticator, go to *Authentication* > *Portals* > *Access Points*, and create a new access point.
2. Enter a name for the access point, and provide the client IP/Hostname from the FortiAP, and click *OK*.

Creating the portal policy on FortiAuthenticator

1. On the FortiAuthenticator, go to *Authentication* > *Portals* > *Policies*, and create a new policy.
   Enter a name for the policy, select *Allow captive portal access*, and choose the previously configured FortiWLC Portal.



2. In Portal selection criteria, configure the following:
   a. *Access points*: Select the previously configured FortiAP access point.
   b. *RADIUS clients*: Select the previously configured FortiWLC RADIUS client.



3. In *Authentication type*, select *Password/OTP authentication* and *Local/remote user*.
4. In *Identity sources*, select the realm for which the user authentication is needed.
5. In *Authentication factors*, select *Verify all configured authentication factors*.
6. Review the RADIUS response and save your changes.

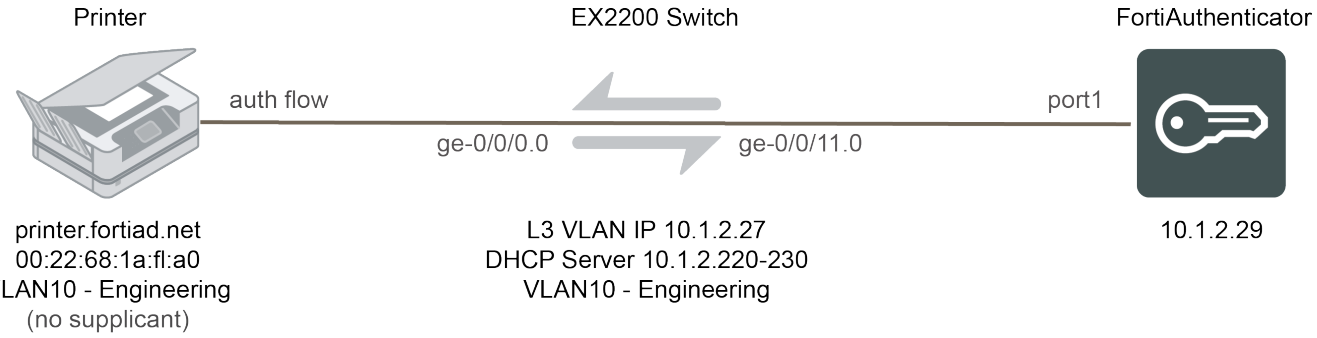
Results

1. Connect a client to the SSID created on the FortiWLC, then log in to the portal with the correct username and password.
   On the FortiAuthenticator, you can go to *Authentication* > *User Management* > *Local Users* to create local user accounts.
2. To confirm the successful log in, on FortiAuthenticator, go to *Logging* > *Log Access* > *Logs*.
3. To confirm the successful log in, on FortiWLC, go to *Monitor* > *Devices* > *All Stations* and find the device showing the authenticated user.

MAC authentication bypass

This section describes configuring MAC address bypass with FortiAuthenticator.

MAC authentication bypass with dynamic VLAN assignment

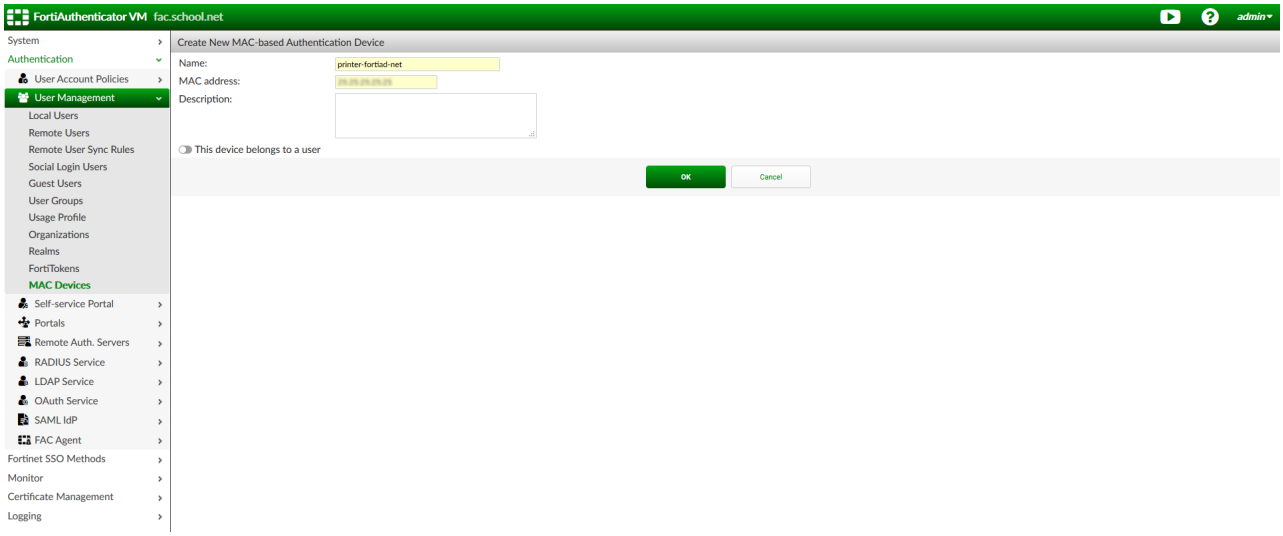


In this recipe, you will configure MAC authentication bypass (MAB) in a wired network with dynamic VLAN assignment.

The purpose of this recipe is to configure and demonstrate MAB with FortiAuthenticator, using a 3rd-party switch (EX2200) to confirm cross-vendor interoperability. The recipe also demonstrates dynamic VLAN allocation without a supplicant.

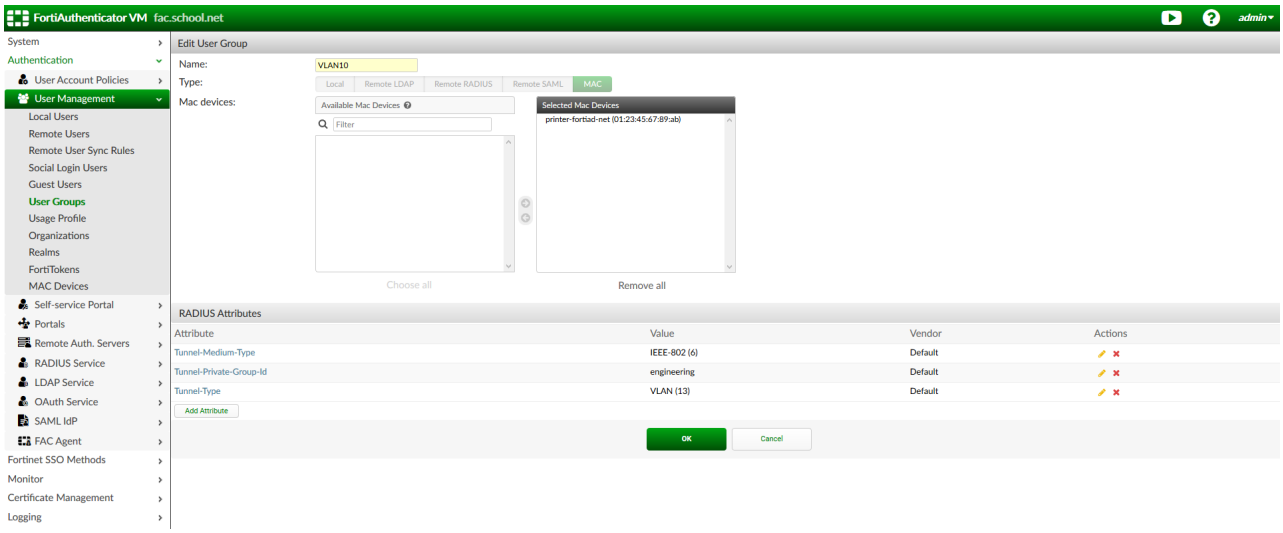
Configuring MAC authentication bypass on the FortiAuthenticator

1. Go to *Authentication* > *User Management* > *MAC Devices* and create a new MAC-based device.
   Enter a name for the device along with the device's MAC address.
   Alternatively, you can use the *Import* option to import this information from a CSV file.



Configuring the user group

1. Go to *Authentication* > *User Management* > *User Groups* and create a new user group. Select *MAC* as the type, and add the newly created MAC device. Click *OK*.
2. Enter the *RADIUS Attributes* as shown in the image below.

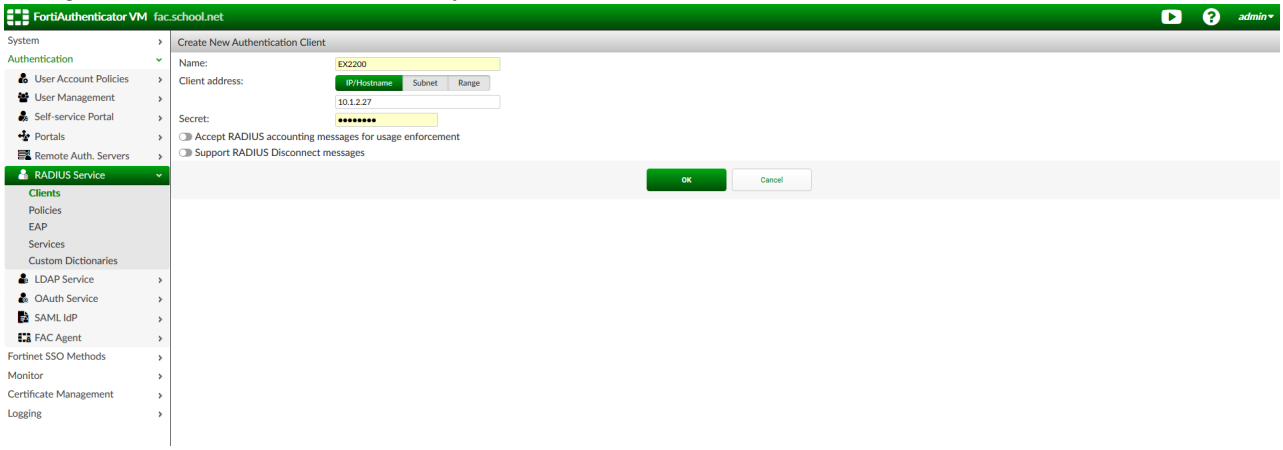


RADIUS attributes can only be added after the group has been created.

Configuring RADIUS settings on FortiAuthenticator

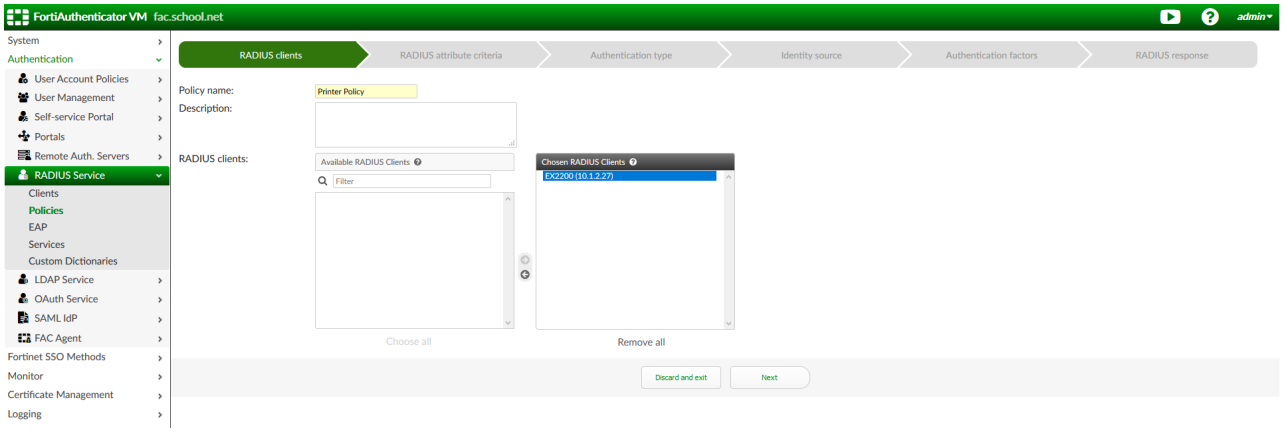
To create the RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients* and create a new RADIUS client. Configure the IP and shared secret from your switch, and click *OK*.



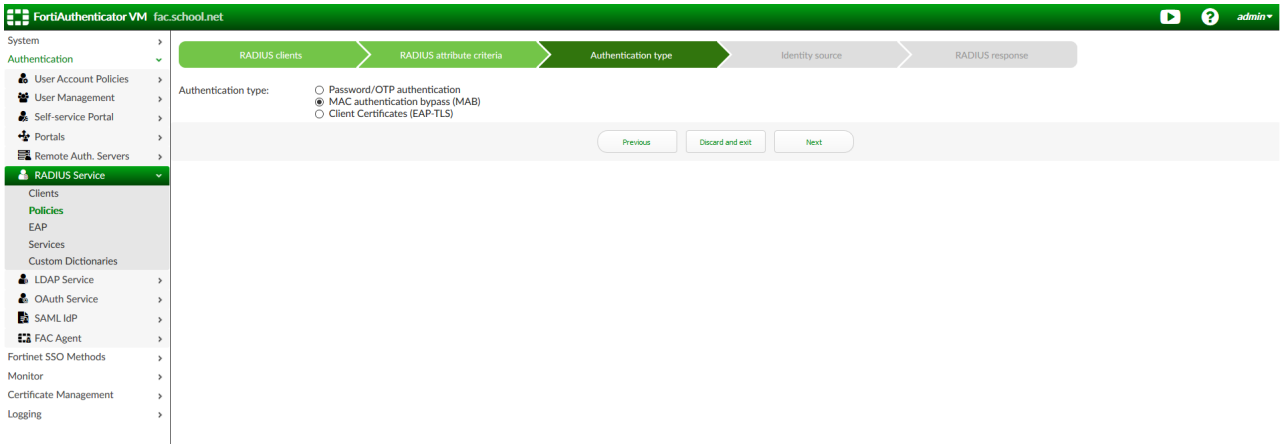
To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies* and create a new RADIUS policy.
   In *RADIUS clients*, enter a policy name, and add the previously configured RADIUS client.

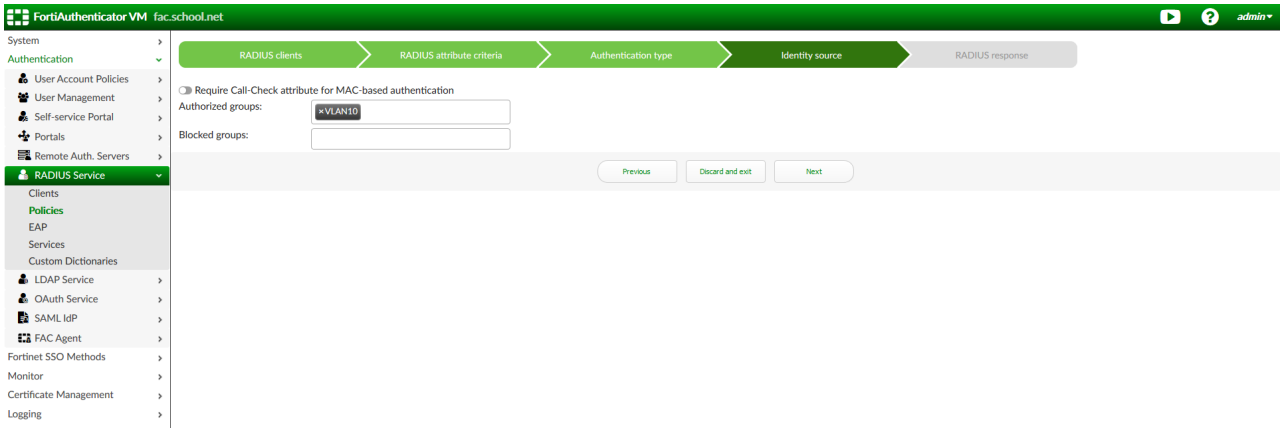


   RADIUS attribute criteria can be left blank.

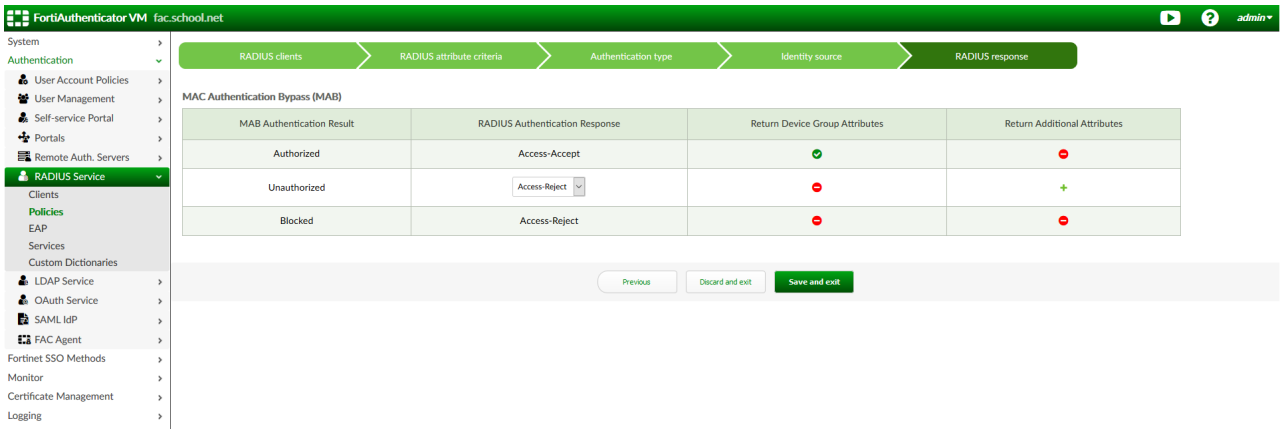
2. In *Authentication type*, select *MAC authentication bypass (MAB)*.



3. In *Identity source*, add the previously configured MAC group to *Authorized groups*.



4. Configure the RADIUS response to reject unauthorized requests, and click *Save and exit*.



Configuring the 3rd-party switch

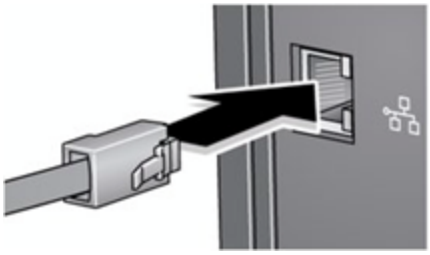
The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

```
set system services dhcp pool 10.1.2.0/24 address-range low 10.1.2.220
set system services dhcp pool 10.1.2.0/24 address-range high 10.1.2.230
set system services dhcp pool 10.1.2.0/24 domain-name fortiad.net
set system services dhcp pool 10.1.2.0/24 name-server 10.1.2.122
set system services dhcp pool 10.1.2.0/24 router 10.1.2.1
set system services dhcp pool 10.1.2.0/24 server-identifier 10.1.2.27
set interfaces ge-0/0/0 unit 0 family ethernet-switching #no vlan assigned to printer
     port, this will be allocated based on Group attributes
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members engineering
     #interface used to communicate with FortiAuthenticator
set interfaces vlan unit 10 family inet address 10.1.2.27/24
set protocols dot1x authenticator authentication-profile-name profile1
set protocols dot1x authenticator interface ge-0/0/0.0 mac-radius restrict #forces mac
     address as username over RADIUS
set access radius-server 10.1.2.29 secret "$9$kmfzIRSlvLhSLNVYZGk.Pf39"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.1.2.29
set vlans engineering vlan-id 10
set vlans engineering l3-interface vlan.10
```

No configuration is required on the endpoint.

Results

1. Connect the wired device (in this case, the printer).



2. Using `tcpdump`, FortiAuthenticator shows receipt of an incoming authentication request (`execute tcpdump host 10.1.2.27 -nnvvXS`):

```
tcpdump: listening on port1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:36:19.110399 IP (tos 0x0, ttl 64, id 18417, offset 0, flags [none], proto UDP (17),
     length 185)
   10.1.2.27.60114 > 10.1.2.29.1812: [udp sum ok] RADIUS, length: 157
      Access-Request (1), id: 0x08, Authenticator: b77fe0657747891fc8d53ae0ad2b0e7a
         User-Name Attribute (1), length: 14, Value: 0022681af1a0 #Switch forces username
              to be endpoint MAC address, no configuration needed on endpoint
            0x0000: 3030 3232 3638 3161 6631 6130
         NAS-Port Attribute (5), length: 6, Value: 70
            0x0000: 0000 0046
         EAP-Message Attribute (79), length: 19, Value: .
            0x0000: 0200 0011 0130 3032 3236 3831 6166 3161
            0x0010: 30
         Message-Authenticator Attribute (80), length: 18, Value: .y{.j.%..9|es.'x
            0x0000: a679 7b82 6344 2593 f639 7c65 73eb 2778
         Acct-Session-Id Attribute (44), length: 24, value: 802.1x81fa002500078442
            0x0000: 384f 322e 3178 3831 6661 3030 3235 3030
            0x0010: 3037 3834 3432
         NAS-Port-rd Attribute (87), length: 12, Value: ge-0/0/0.0
            0x0000: 6765 2430 2f30 2f30 2e30
         Calling-Station-Id Attribute (31), length: 19, value: 00-22-68-1a-fl-a0
            0x0000: 3030 2032 3220 3638 2031 6120 6631 2461
            0x0010: 30
         Called-Station-Id Attribute (30), length: 19, Value: a8-40-e5-b0-21-80
            0x0000: 6138 2464 3024 6535 2d62 302d 3231 2d38
            0x0010: 30
         NAS-Port-Type Attribute (61), length: 6, value: Ethernet
            0x0000: 0000 000f
```

3. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to verify the device authentication.
   The Debug Log (at `https://<fac-ip>/debug/radius`) should also confirm successful authentication.
4. Continuing with the `tcpdump`, authentication is accepted from FortiAuthenticator and authorization attributes returned to the switch:

```
17:36:19.115264 IP (tos 0x0, ttl 64, id 49111, offset 0, flags [none], proto UDP (17),
     length 73)
   10.1.2.29.1812 > 10.1.2.27.60114: (bad udp cksum 0x1880 -> 0x5ccel] RADIUS, length: 45
      Access-Accept (2), id: 0x08, Authenticator: b5c7b1bb5a316fb483a622eaae58ccc2
         Tunnel-Type Attribute (64), length: 6, Value: Tag[Unused] #13
            0x0000: 0000 000d
         Tunnel-Medium-Type Attribute (65), length: 6, Value: Tag[Unused] 802
            0x0000: 0000 0006
         Tunnel-Private-Group-ID Attribute (81), length: 13, Value: engineering
```

```
        0x0000: 656e 6769 6e65 6572 696e 67
    0x0000: 4500 0049 bfd7 0000 4011 a293 0a01 021d E..I....@ .......
    0x0010: 0a01 021b 0714 ead2 0035 1880 0208 002d 5
    0x0020: b5c7 blbb 5a31 6fb4 83a6 22ea ae58 ccc2 ....21o..."..X..
    0x0030: 4006 0000 0000 4106 0000 0006 510d 656e @ A Q en
    0x0040: 6769 6e65 6572 696e 67 gineering
```

5. Post-authentication DHCP transaction is picked up by FortiAuthenticator

   The Switch CLI shows a successful dot1x session:

```
root# run show dotlx interface ge-0/0/0.0
802.1X Information:
Interface Role State MAC address User
ge-0/0/0.0 Authenticator Authenticated 00:22:68:1A:F1:A0 0022681af1a0
```

   The MAC address interface has been dynamically placed into correct VLAN:

```
root# run show vlans engineering
Name Tag Interfaces
engineering 10
     ge-0/0/0.0*, ge-0/0/11.0*
```

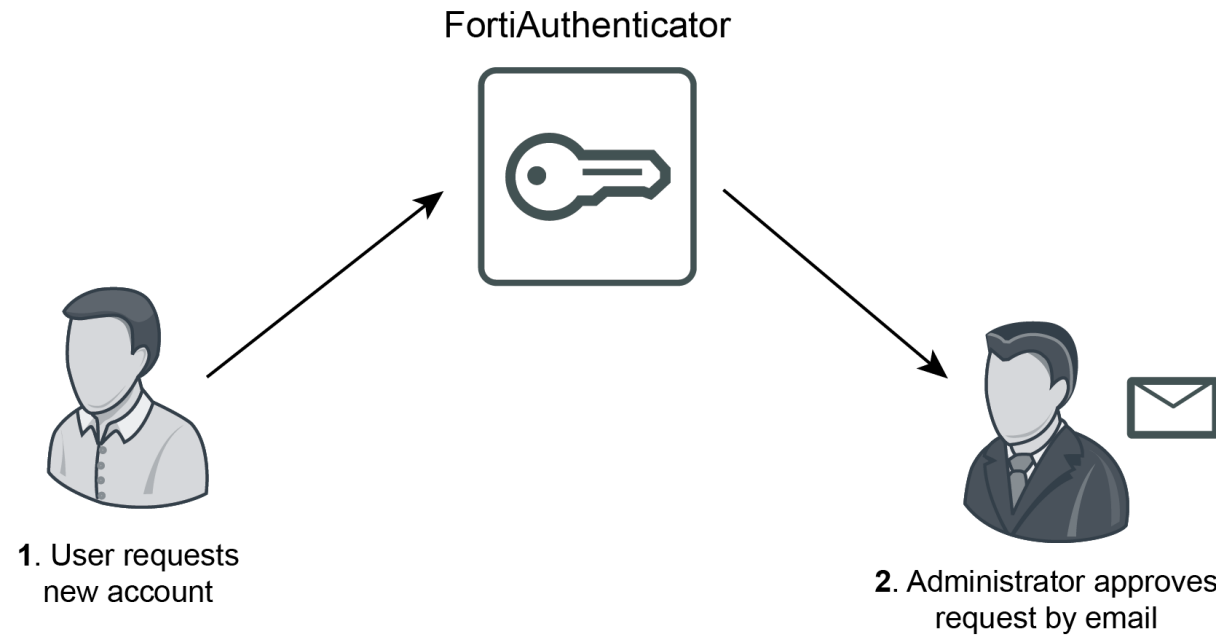
   Additionally, the printer shows as available on the network:

```
root# run show arp interface vlan.10
MAC Address Address Name Interface Flags
00:0c:29:5b:90:68 10.1.2.29 10.1.2.29 vlan.10 none
6c:70:9f:d6:ae:al 10.1.2.220 10.1.2.220 vlan.10 none
b8:53:ac:4a:d5:f5 10.1.2.221 10.1.2.221 vlan.10 none
00:22:68:1a:fl:a0 10.1.2.224 10.1.2.224 vlan.10 none
a4:c3:61:24:b9:07 10.1.2.228 10.1.2.228 vlan.10 none
Total entries: 5

{master:0}[edit]
root* run ping 10.1.2.224
PING 10.1.2.224 (10.1.2.224): 56 data bytes
64 bytes from 10.1.2.224: icmp_seq=0 tt1=128 time=2.068 ms
64 bytes from 10.1.2.224: icmp_seq=1 tt1=128 time=2.236 ms
64 bytes from 10.1.2.224: icmp_seq=2 tt1=128 time=2.699 ms

--- 10.1.2.224 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.068/2.334/2.699/0.267 ms
```

Self-service Portal

Configure general self-service portal options, including access control settings, self-registration options, replacement messages, and device self-enrollment settings.

FortiAuthenticator user self-registration



For this recipe, you will configure the FortiAuthenticator self-service portal to allow users to add their own account and create their own passwords.

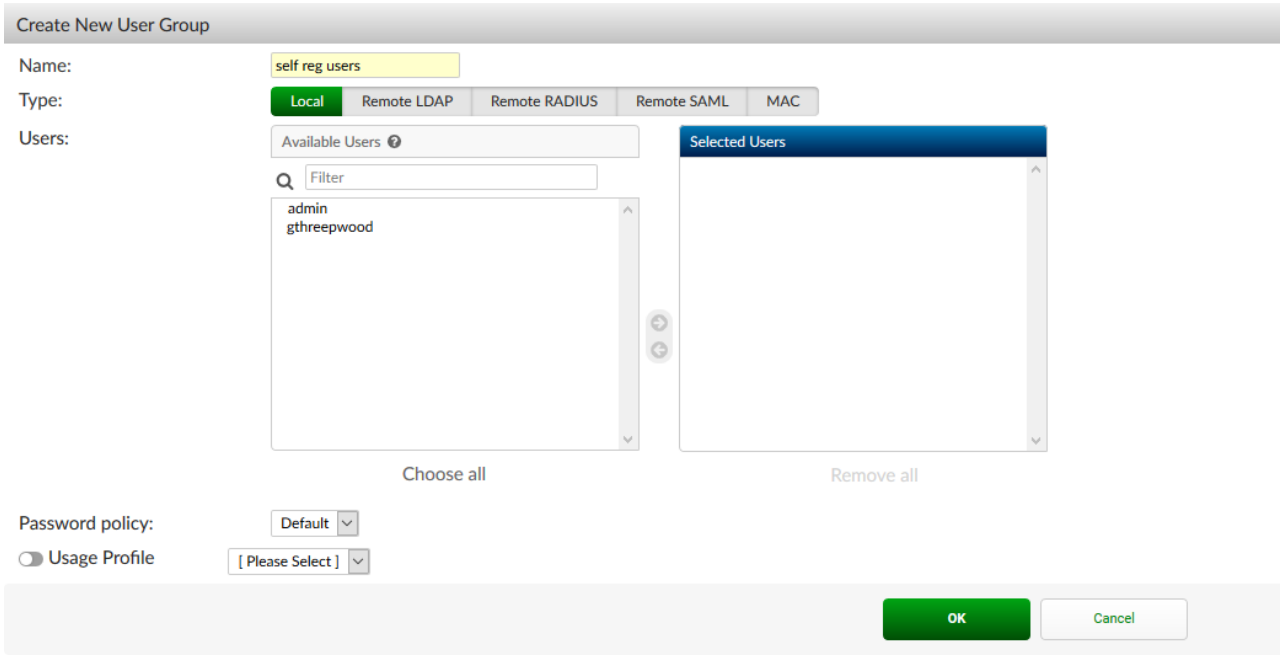
Note that enabling and using administrator approval requires the use of an email server, or SMTP server. Since administrators will approve requests by email, this recipe describes how to add an email server to your FortiAuthenticator. You will create and use a new server instead of the unit's default server.

Creating a self-registration user group

To create a self-registration user group:

1. Go to *Authentication* > *User Management* > *User Groups* and create a new user group for self-registering users. Enter a *Name* and select *OK*. Users will be added to this group once they register through the self-registration

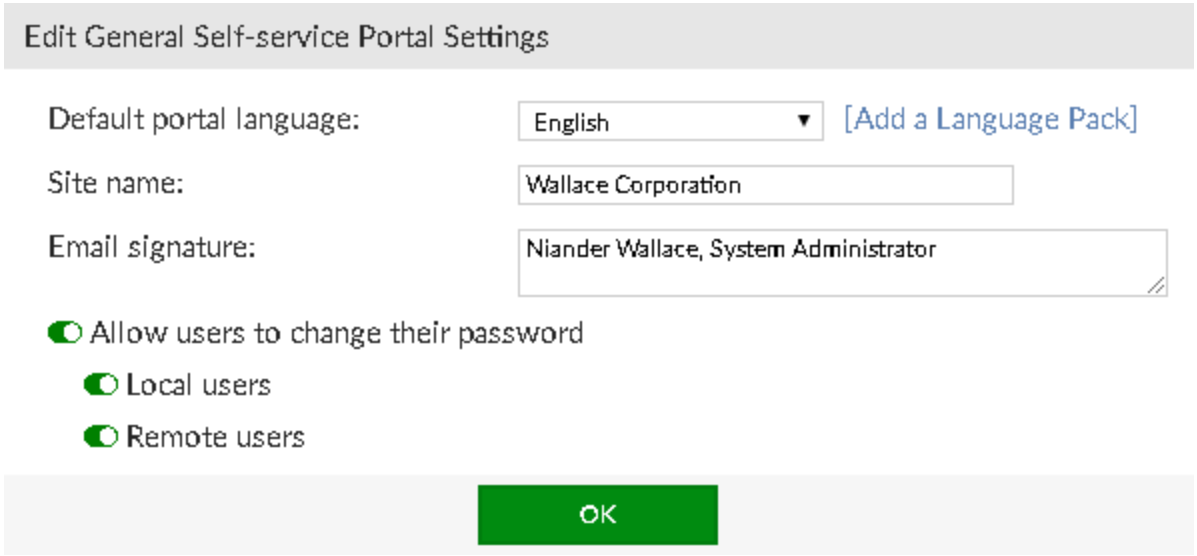
portal.



Enabling self-registration

To enable self-registration:

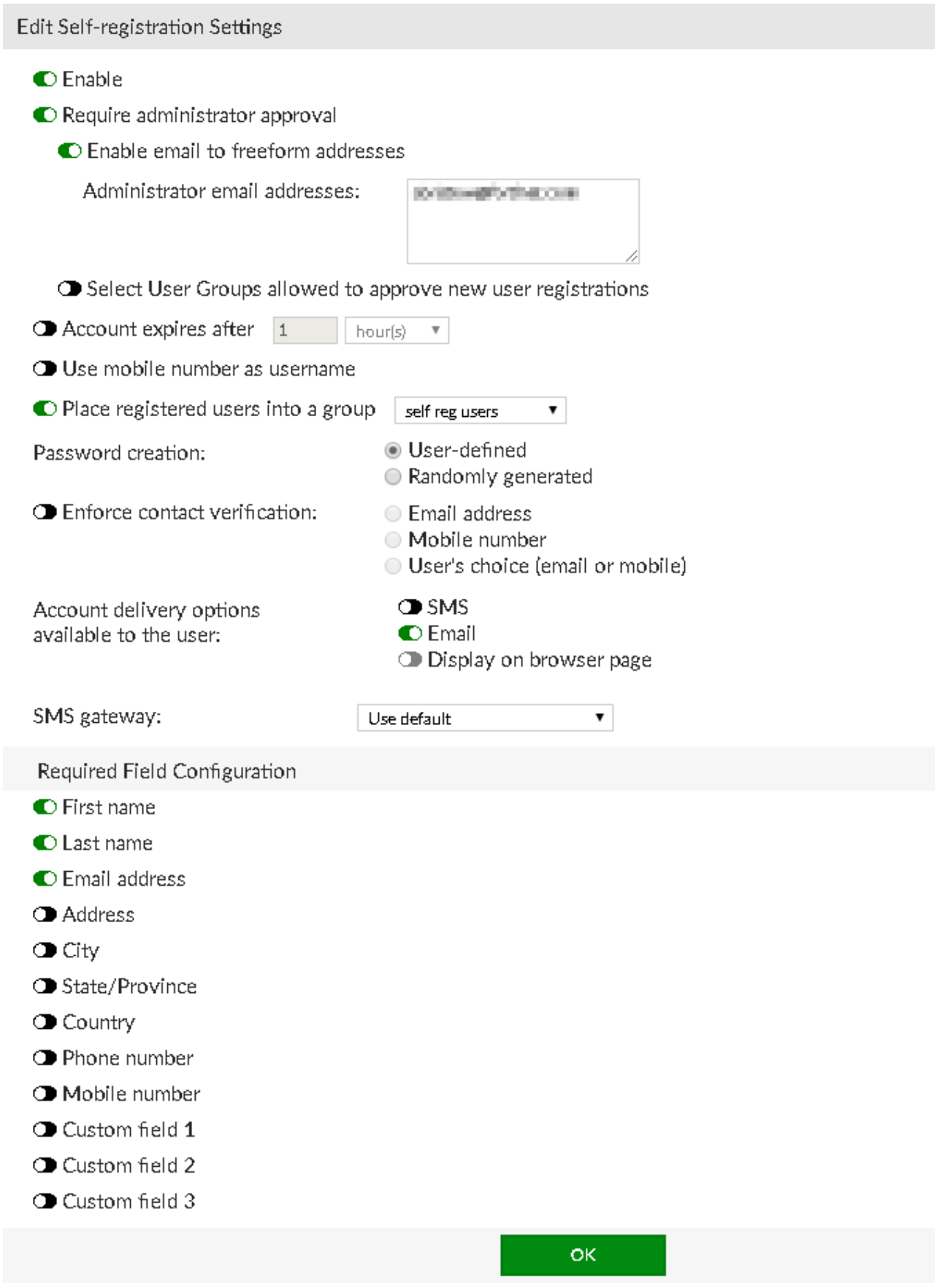
1. Go to *Authentication* > *Self service Portal* > *General*.
   Enter a *Site name*, add an *Email signature* that you would like appended to the end of outgoing emails, and select *OK*.



2. Then go to *Authentication* > *Self-service Portal* > *Self-registration* and select *Enable*.
   Enable *Require administrator approval* and *Enable email to freeform addresses*, and enter the administrator's email address in the field provided.

Enable *Place registered users into a group*, select the user group created earlier, and configure basic account information to be sent to the user by *Email*.

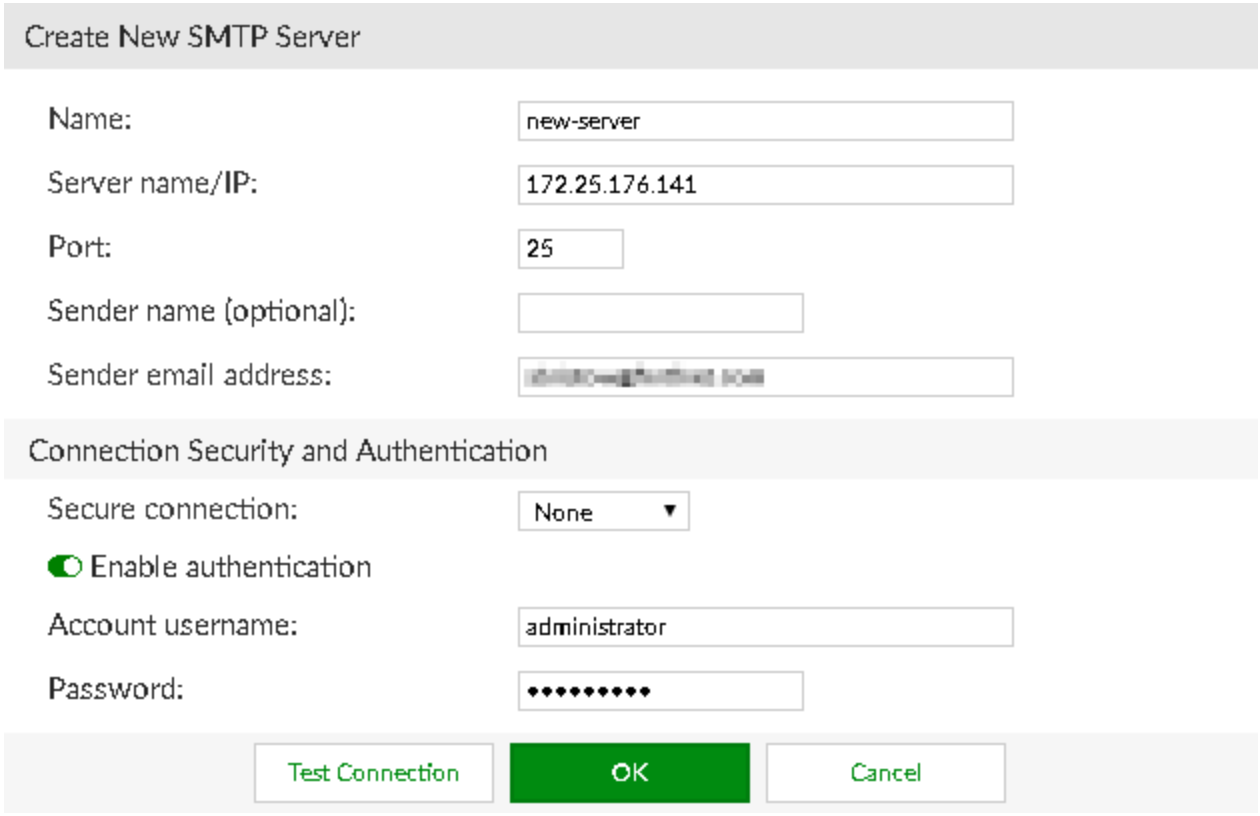
Open the *Required Field Configuration* dropdown and enable *First name*, *Last name*, and *Email address*.


Edit Self-registration Settings
Enable
Require administrator approval
Enable email to freeform addresses
Administrator email addresses:
Select User Groups allowed to approve new user registrations
Account expires after
1
hour(s)
Use mobile number as username
Place registered users into a group
self reg users
Password creation:
User-defined
Randomly generated
Enforce contact verification:
Email address
Mobile number
User's choice (email or mobile)
Account delivery options available to the user:
SMS
Email
Display on browser page
SMS gateway:
Use default
Required Field Configuration
First name
Last name
Email address
Address
City
State/Province
Country
Phone number
Mobile number
Custom field 1
Custom field 2
Custom field 3
OK

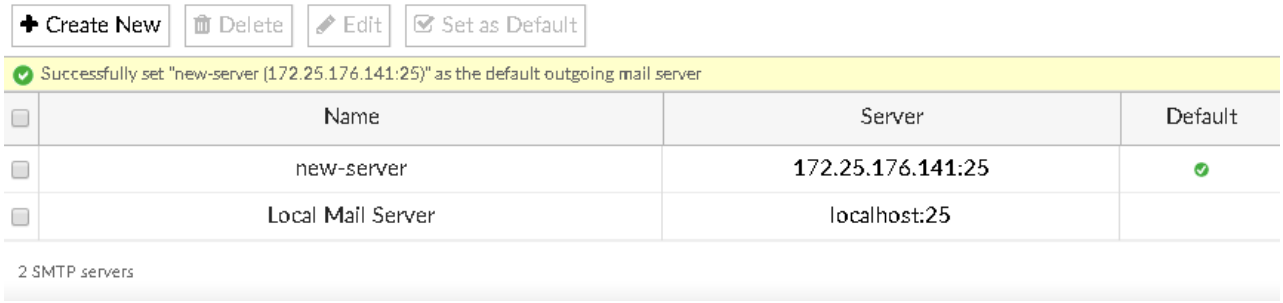
Creating a new SMTP server

To create a new SMTP server:

1. Go to *System* > *Messaging* > *SMTP Servers* and create a new email server for your users.
   Enter a *Name*, the IP address of the FortiAuthenticator, and leave the default port value (`25`).
   Enter the administrator's email address, *Account username*, and *Password*.
   Note that, for the purpose of this recipe, *Secure connection* will not be set to *STARTTLS* as a signed CA certificate would be required.

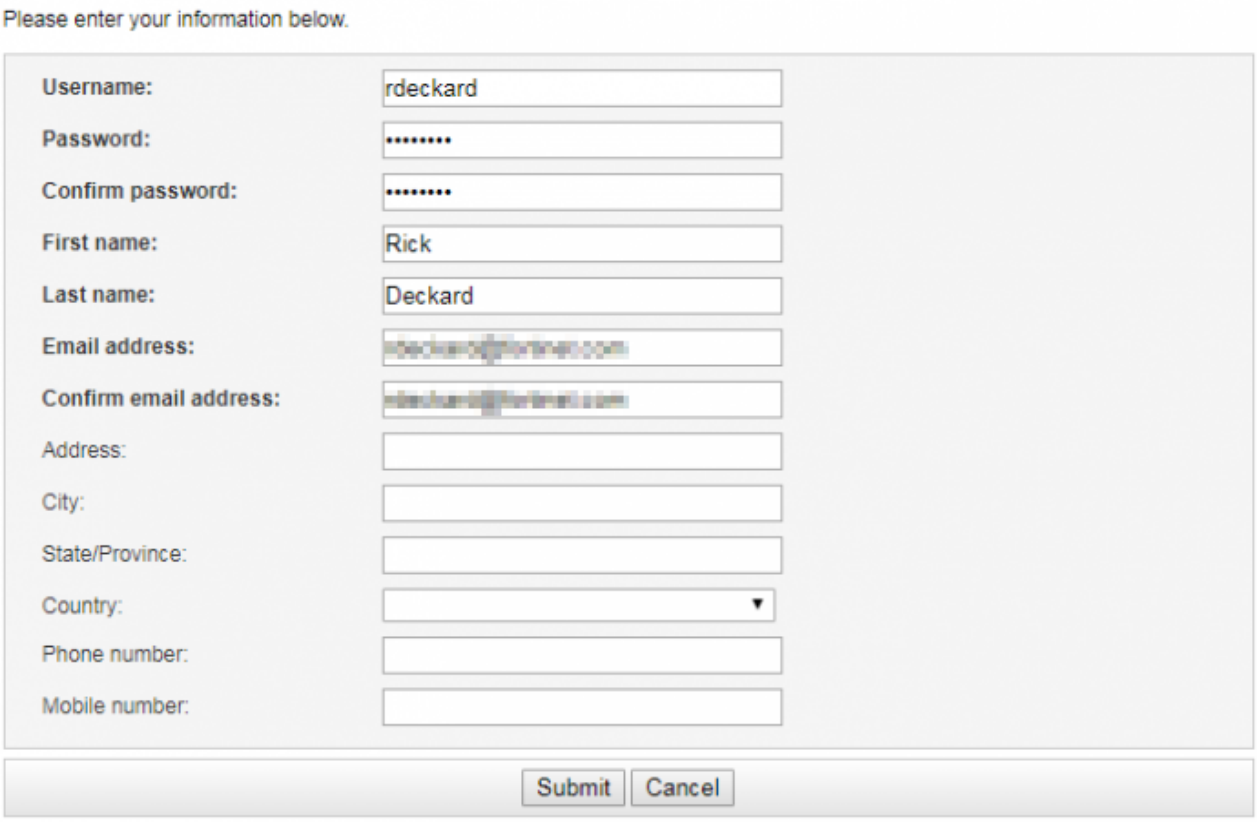


2. Once created, highlight the new server and select *Set as Default*.
   The new SMTP server will now be used for future user registration.

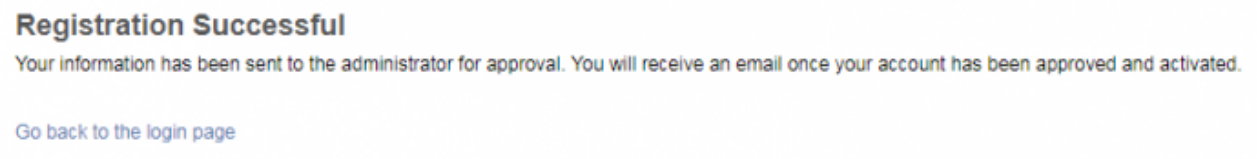


Results - Self-registration

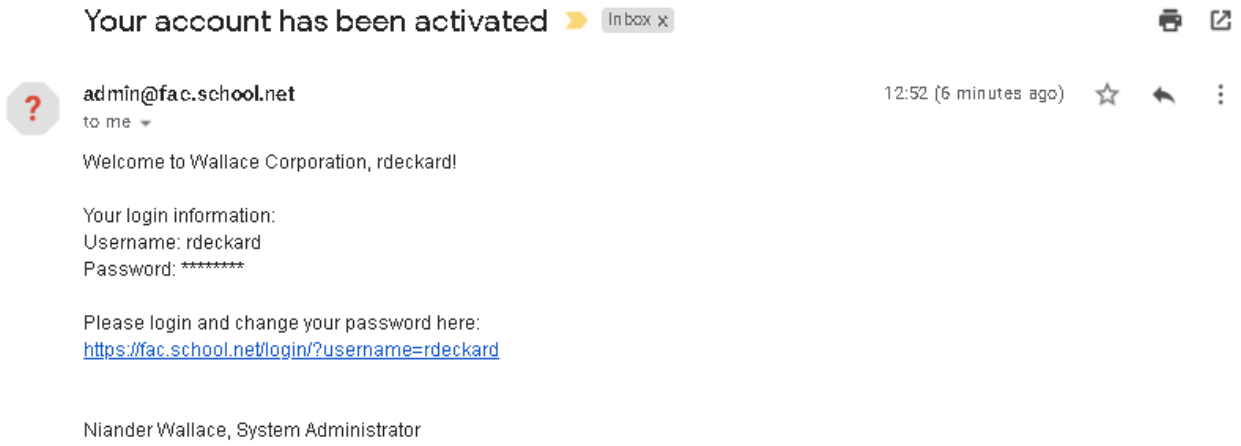
1. When the user visits the login page, *https://<FortiAuthenticator-IP>/auth/register/*, they can click the *Register* button, where they will be prompted to enter their information.
   They will need to enter and confirm a *Username*, *Password*, *First name*, *Last name*, and *Email address*. These are the only required fields, as configured in the FortiAuthenticator earlier.
   Select *Submit*.



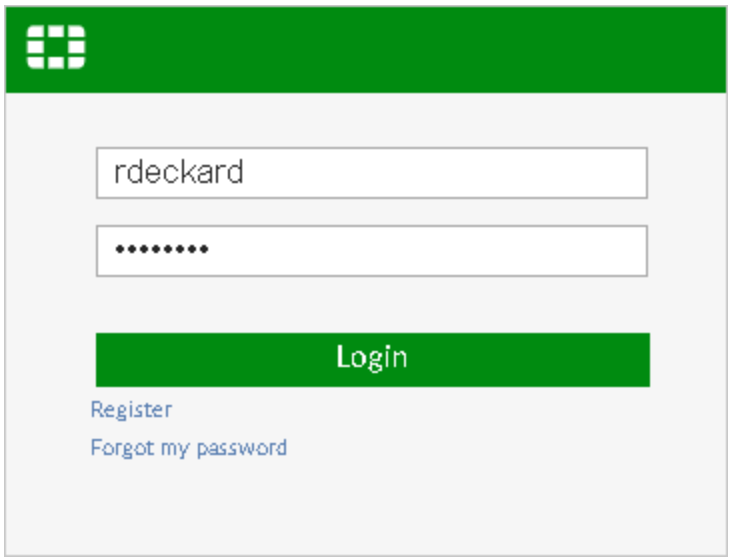
2. The user's registration is successful, and their information has been sent to the administrator for approval.



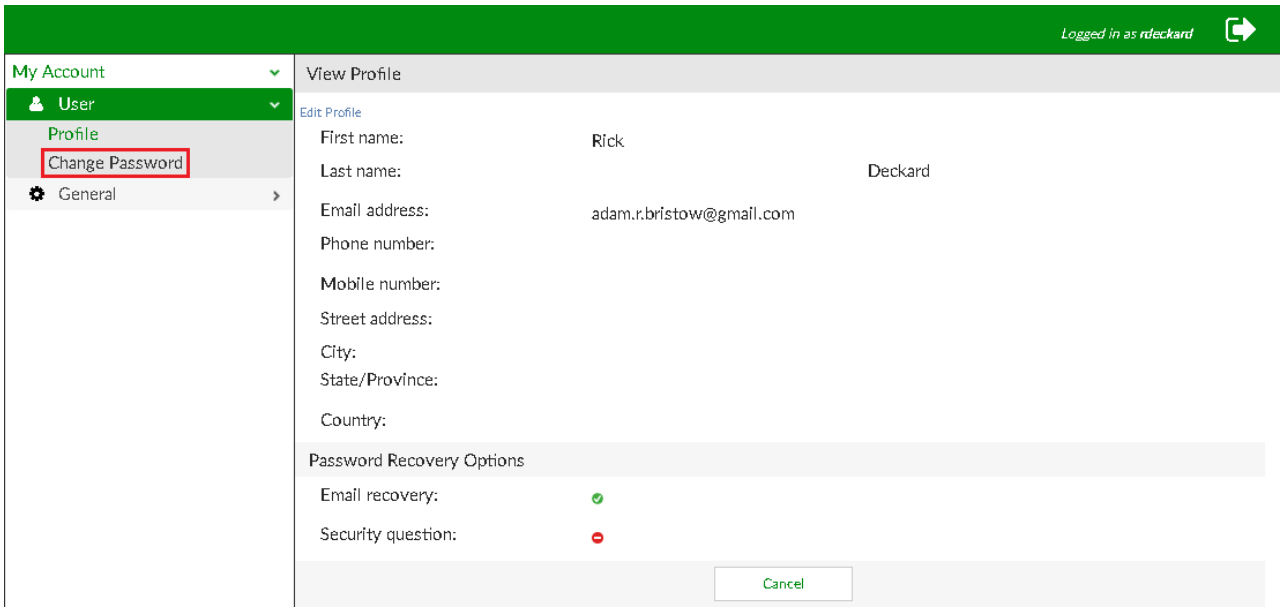
3. When the administrator has enabled the user's account, the user will receive an activation welcome email.
   The user's login information will be listed.



4. Select the link and log in to the user's portal.

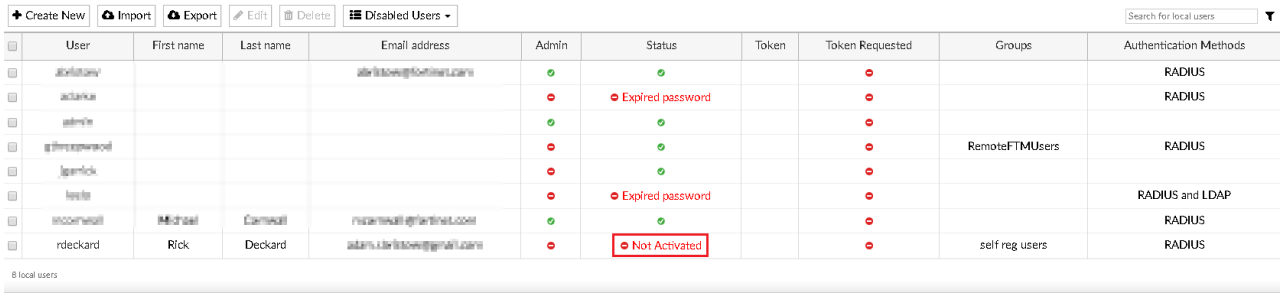


5. The user is now logged into their account where they can review their information.
As recommended in the user's welcome email, the user may change their password. However, this is optional.

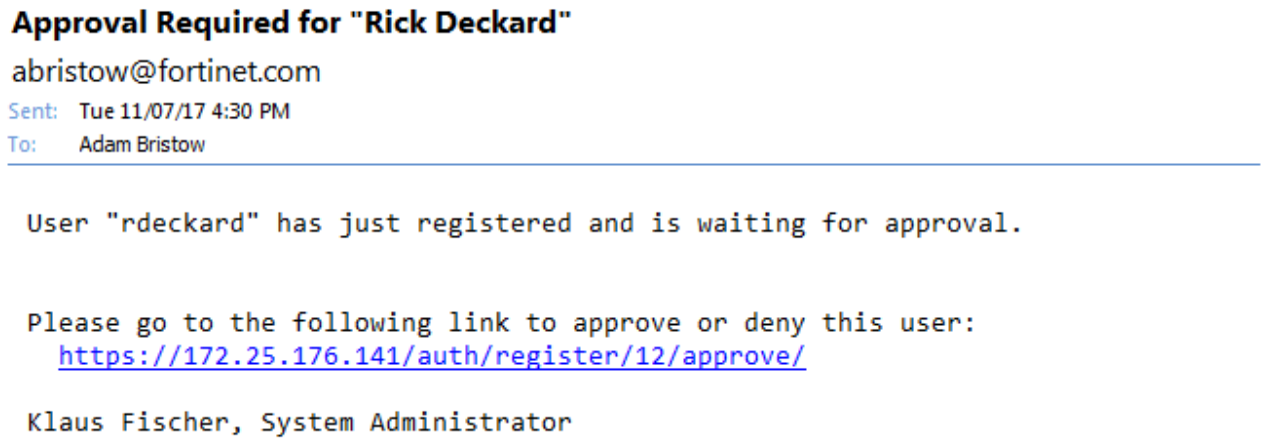


Results - Administrator approval

1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to *Authentication > User Management > Local Users*. The user has been added, but their *Status* is listed as *Not Activated*.



2. In the administrator's email account, open the user's *Approval Required* email. The user's full name will appear in the email's subject, along with their username in the email's body.
   Select the link to approve or deny the user.



Approval Required for "Rick Deckard"

abristow@fortinet.com

Sent: Tue 11/07/17 4:30 PM

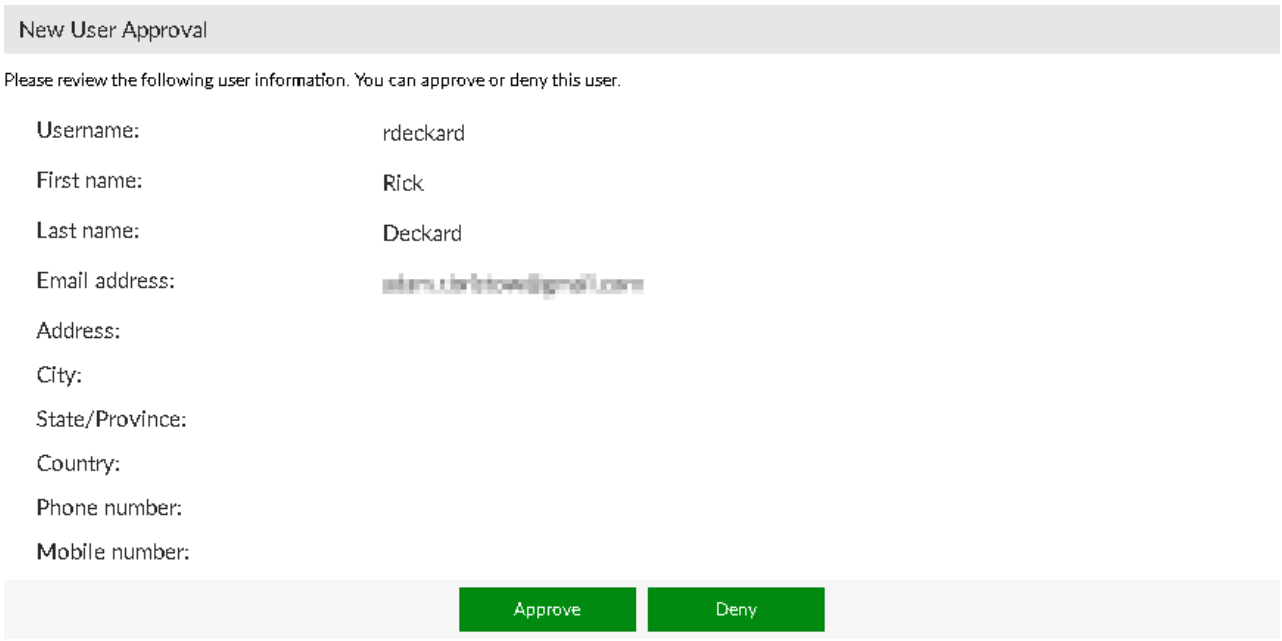
To: Adam Bristow

User "rdeckard" has just registered and is waiting for approval.

Please go to the following link to approve or deny this user:
https://172.25.176.141/auth/register/12/approve/

Klaus Fischer, System Administrator

3. The link will take you to the *New User Approval* page, where you can review the user's information and either approve or deny the user's full registration.
Select *Approve*.



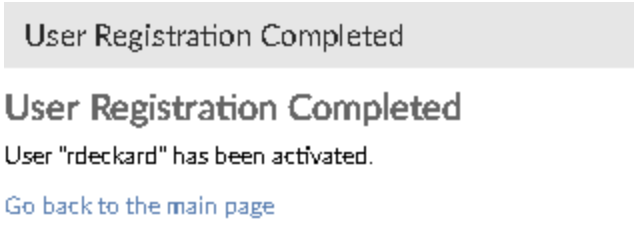
New User Approval

Please review the following user information. You can approve or deny this user.

Username:	rdeckard
First name:	Rick
Last name:	Deckard
Email address:	[redacted]
Address:	
City:	
State/Province:	
Country:	
Phone number:	
Mobile number:	

Approve Deny

4. The user has now been approved and activated by the administrator.



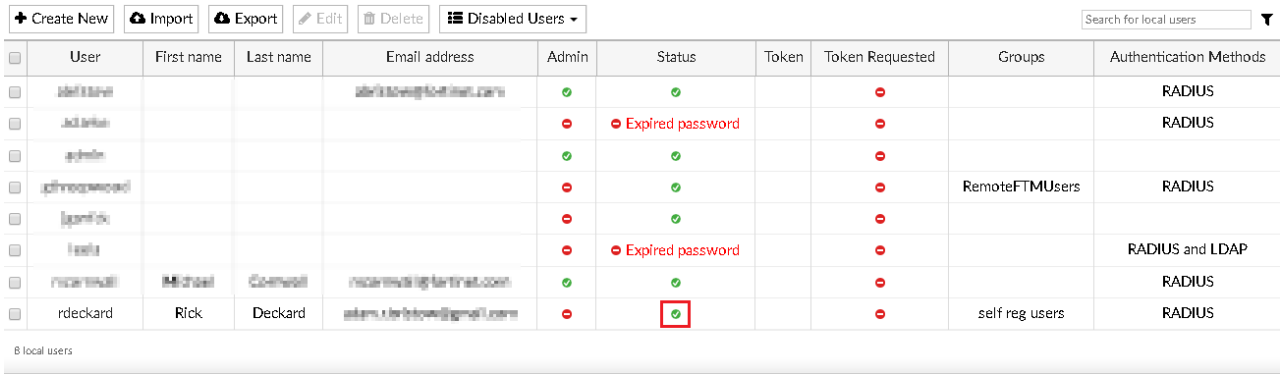
User Registration Completed

User Registration Completed

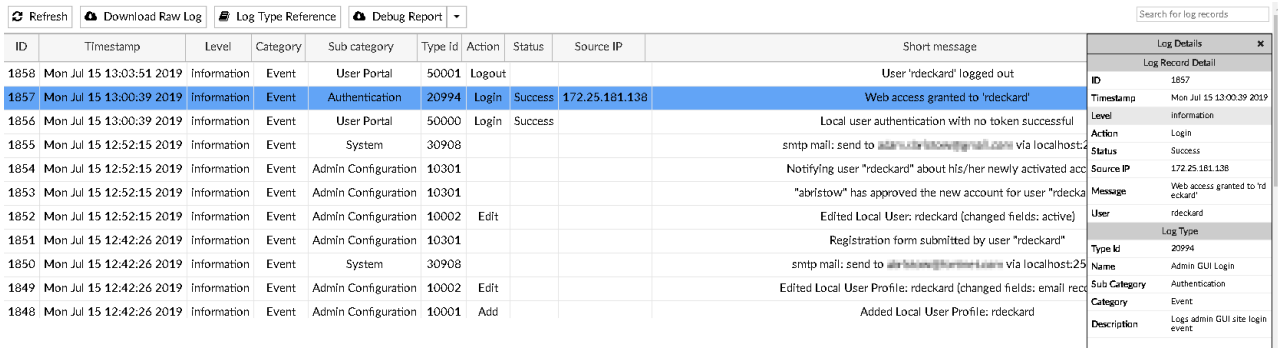
User "rdeckard" has been activated.

Go back to the main page

This can be confirmed by going back to *Authentication* > *User Management* > *Local Users*. The user's **Status** has changed to **Enabled**.



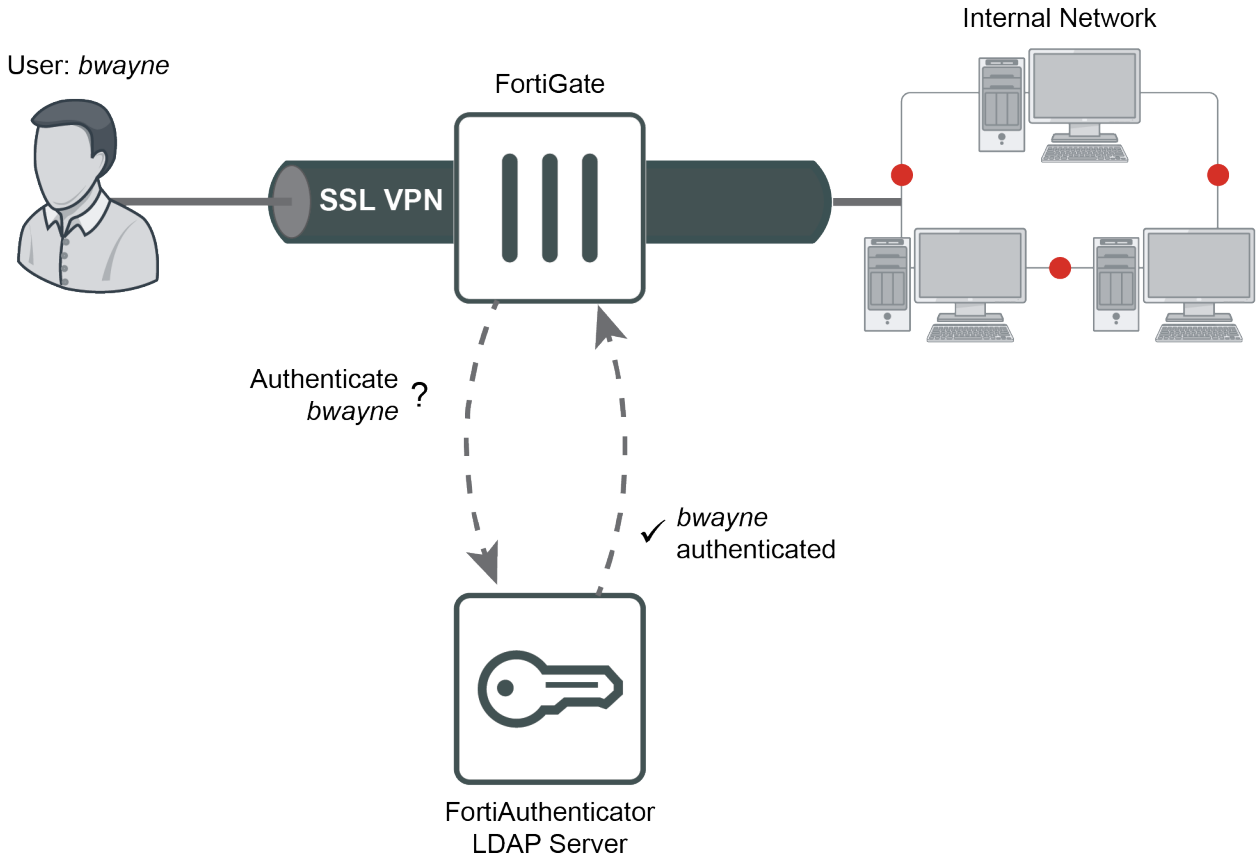
5. You can also go to *Logging* > *Log Access* > *Logs* to view the successful login of the user and more information.



VPNs

This section contains information about creating and using a virtual private network (VPN).

LDAP authentication for SSL VPN with FortiAuthenticator



This recipe describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an LDAP server.

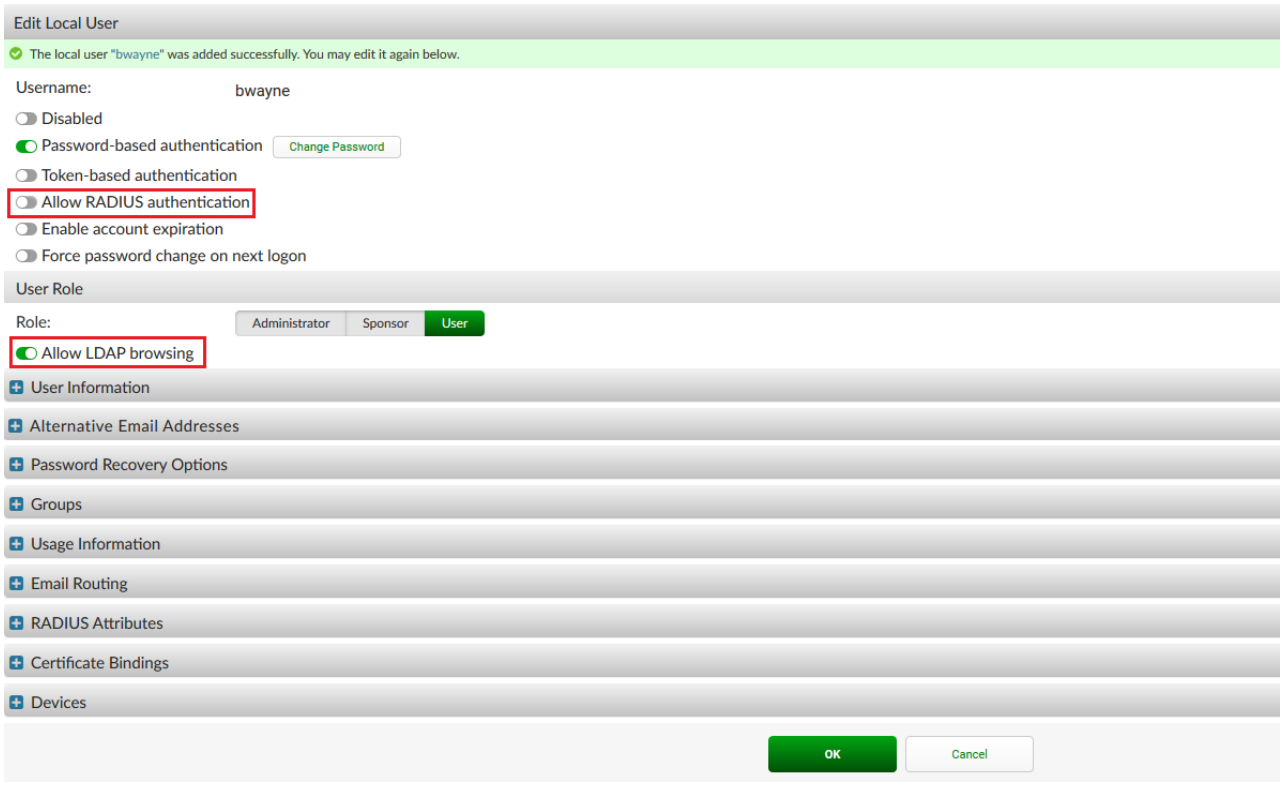
Creating the user and user group on the FortiAuthenticator

To create the user and user group:

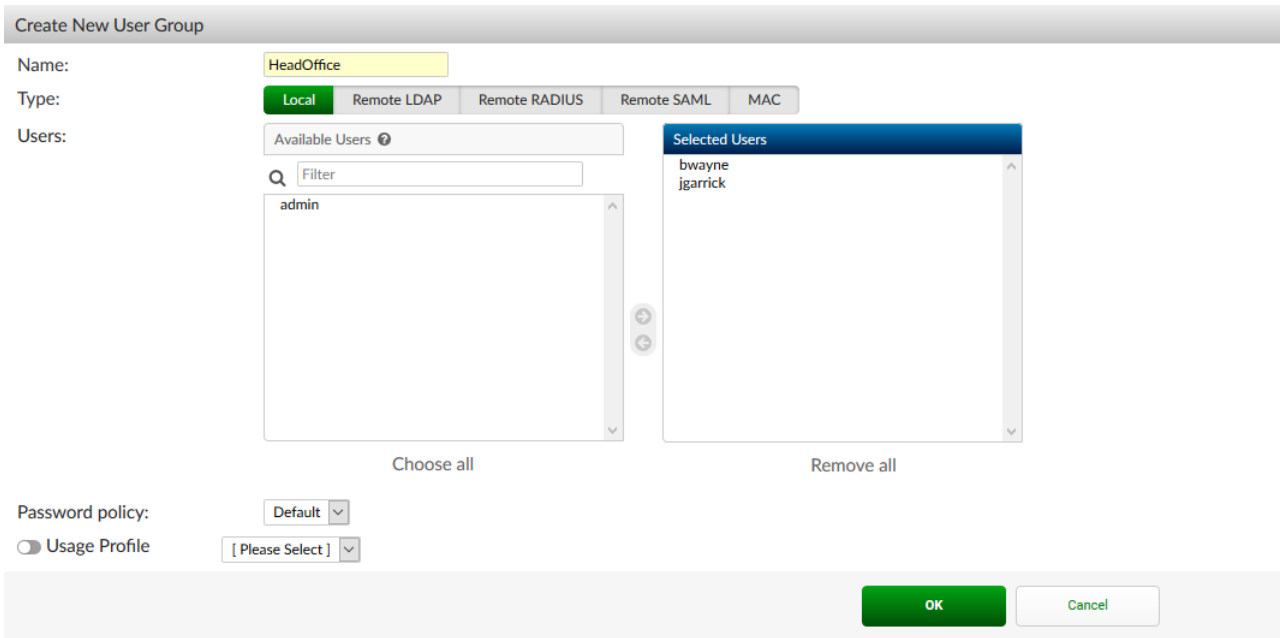
1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and select *Create New*. Enter a name for the user, enter and confirm a password, and be sure to disable *Allow RADIUS authentication* — RADIUS authentication is not required for this recipe.

   Set *Role* as *User*, and select *OK*. New options will appear.

Make sure to enable *Allow LDAP browsing* — the user will not be able to connect to the FortiGate otherwise.



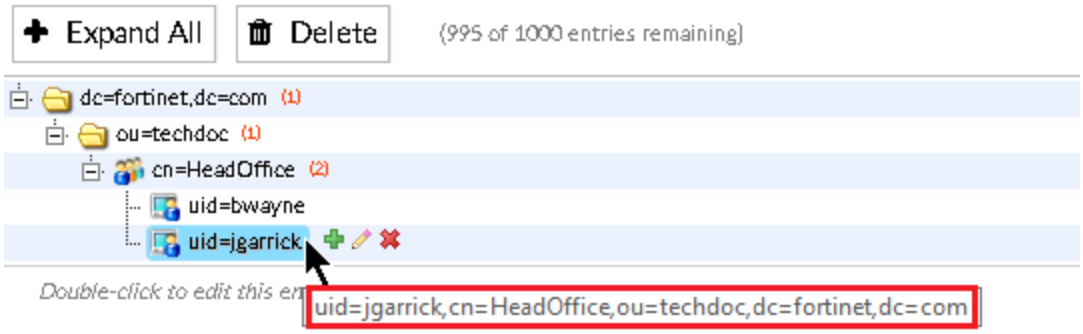
2. Create another user with the same settings. Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.
3. Next go to *Authentication* > *User Management* > *User Groups*, and create a user group for the FortiGate users. Add the desired users to the group.



Creating the LDAP directory tree on the FortiAuthenticator

To create the LDAP directory tree:

1. Go to *Authentication* > *LDAP Service* > *Directory Tree*, and create a Distinguished Name (DN). A DN is made up of Domain Components (DC).
   Both the users and user group created earlier are the User ID (UID) and the Common Name (CN) in the LDAP Directory Tree.
   Create an Organizational Unit (OU), and a Common Name (CN). Under the *cn=HeadOffice* entry, add UIDs for the users.
   If you mouse over a user, you will see the full DN of the LDAP server.

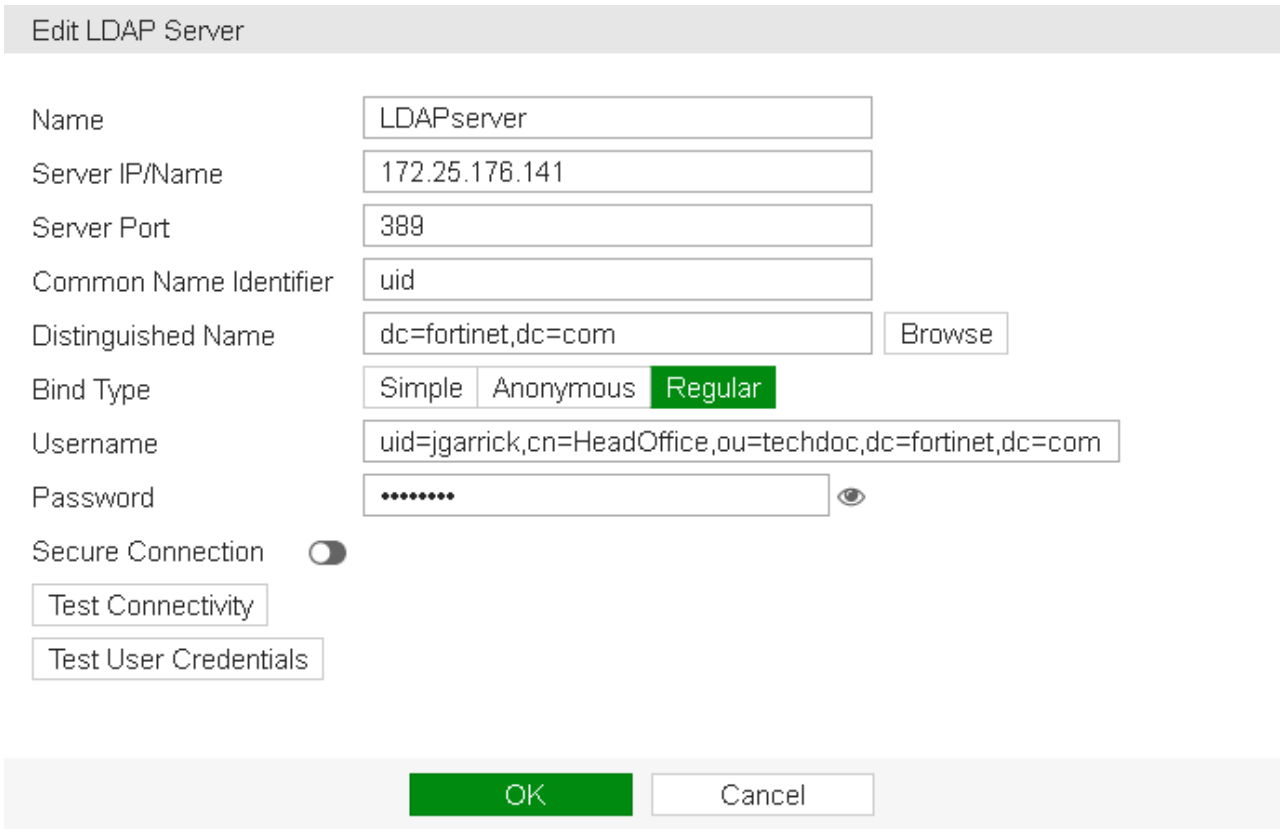


   Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.

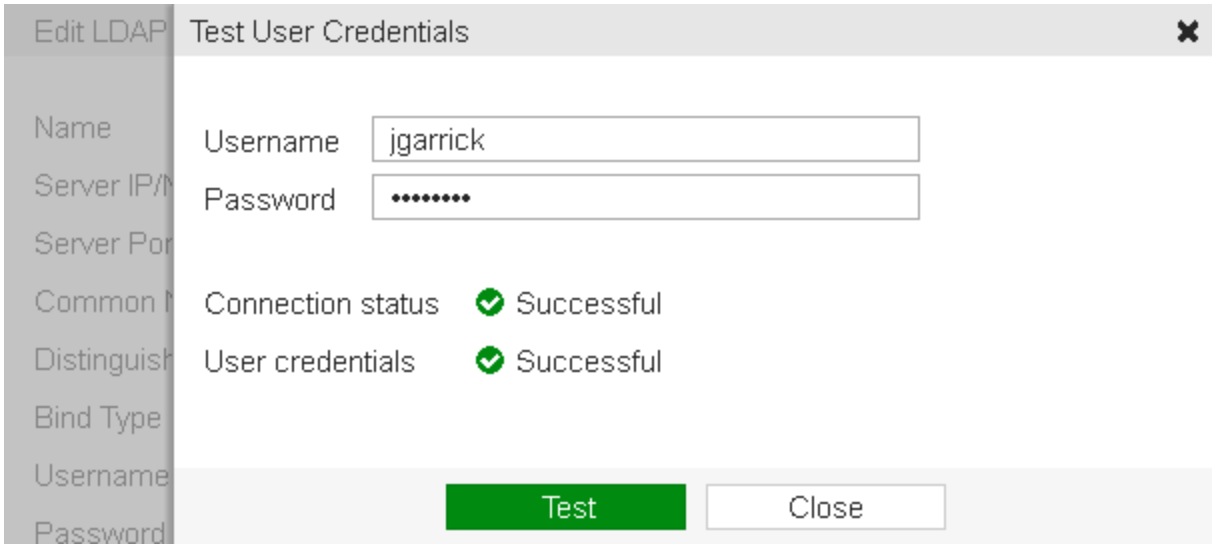
Connecting the FortiGate to the LDAP server

To connect the FortiGate to the LDAP server:

1. On the FortiGate, go to *User & Device* > *LDAP Servers*, and select *Create New*.
   Enter a name for the LDAP server connection.
   Set *Server IP/Name* to the IP of the FortiAuthenticator, and set the *Common Name Identifier* to *uid*.
   Set *Distinguished Name* to `dc=fortinet,dc=com`, and set the *Bind Type* to *Regular*.
   Enter the user DN for jgarrick of the LDAP server, and enter the user's *Password*.
   The DN is an account that the FortiGate uses to query the LDAP server.



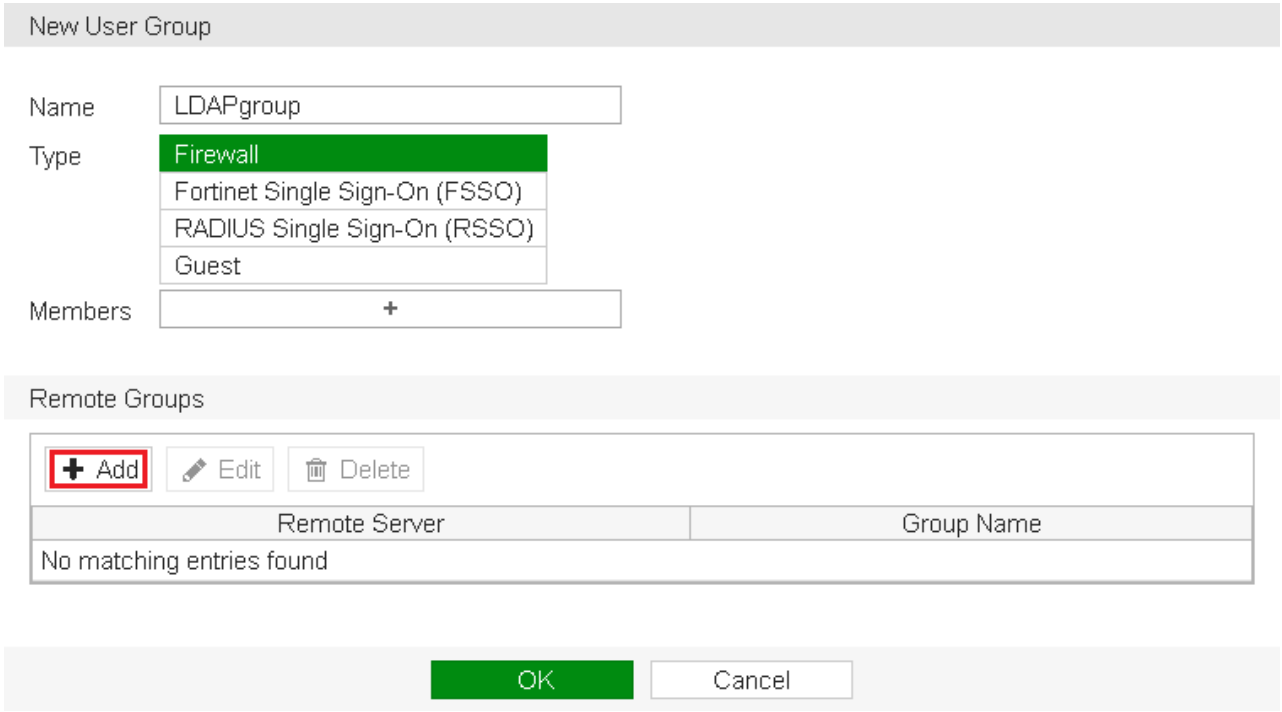
2. Select *Test Connectivity* to determine a successful connection.
Then select *Test User Credentials* to query the LDAP directory using jgarrick's credentials. The query is successful.



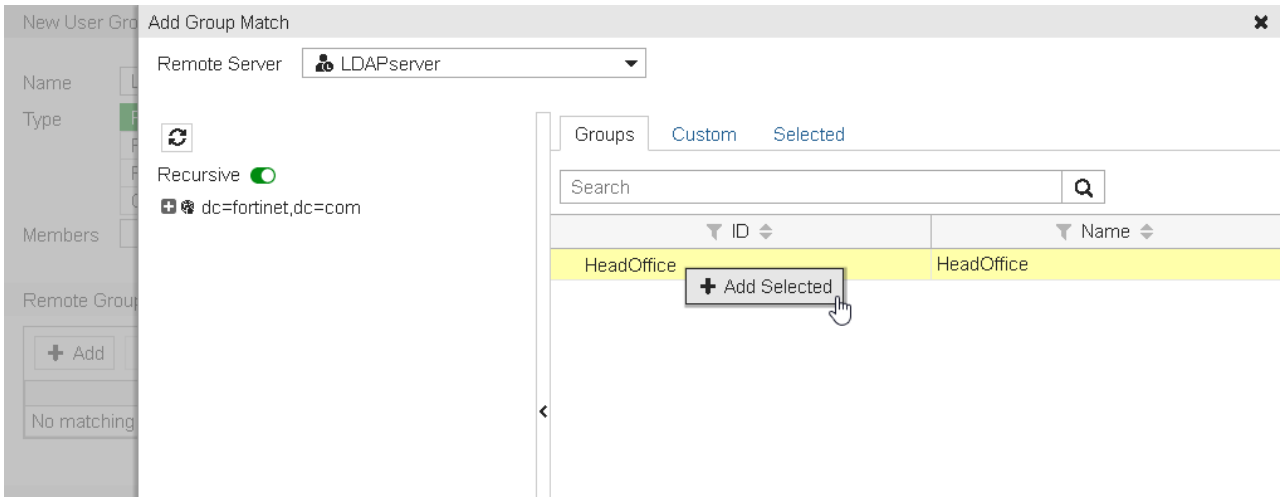
Creating the LDAP user group on the FortiGate

To create the LDAP user group:

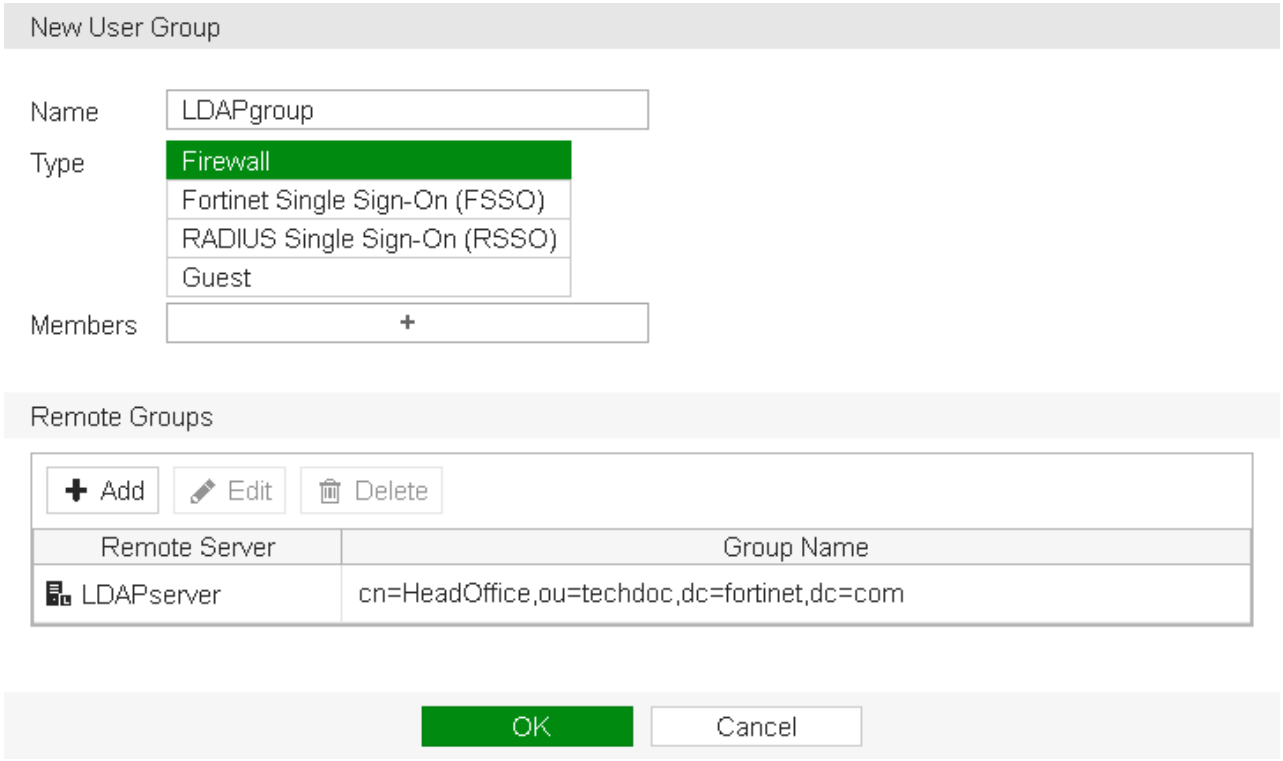
1. Go to *User & Device* > *User Groups*, and select *Create New*.
   Enter a name for the user group. Under *Remote Groups* select *Add*.



2. Select *LDAPserver* under the *Remote Server* dropdown.
   In the new *Add Group Match* window, right-click *HeadOffice* under the *Groups* tab, and select *Add Selected*. The group will be added to the *Selected* tab. Select *OK*.



3. *LDAPserver* has been added to the LDAP group. Select *OK*.



Configuring the SSL-VPN

To configure the SSL-VPN:

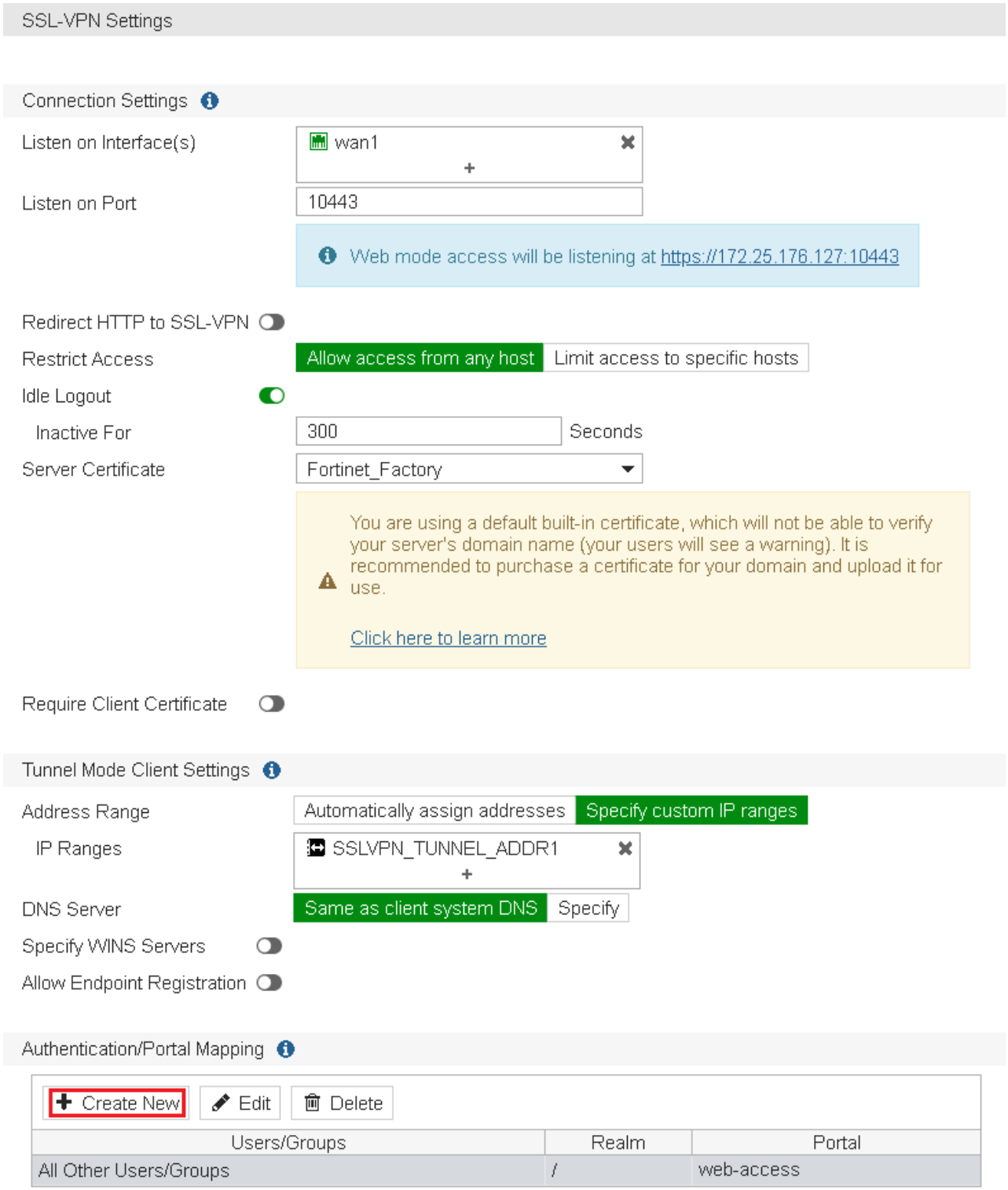
1. On the FortiGate, go to *VPN* > *SSL-VPN Portals*, and edit the full-access portal. Disable *Split Tunneling*.

2. Go to *VPN* > *SSL-VPN Settings*.

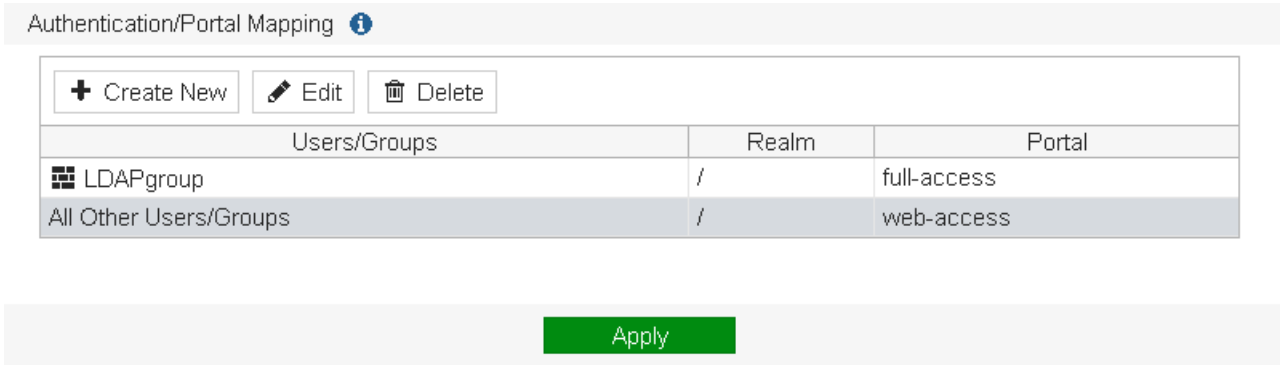
Under *Connection Settings* set *Listen on Port* to `10443`.

Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set it to *SSLVPN_TUNNEL_ADDR1*.

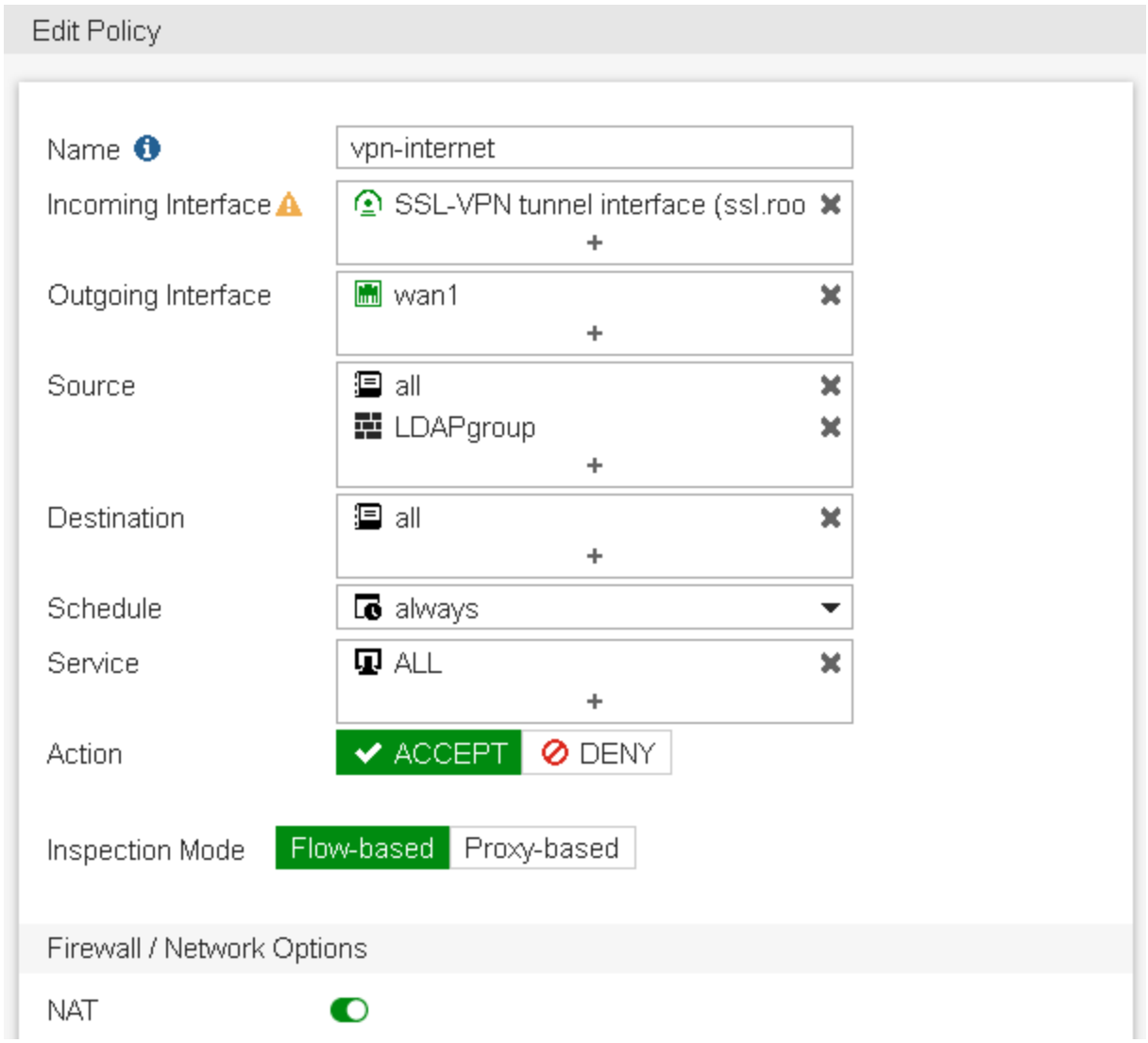
Under *Authentication/Portal Mapping*, select *Create New*.



3. Assign the *LDAPgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal. Select *Apply*.

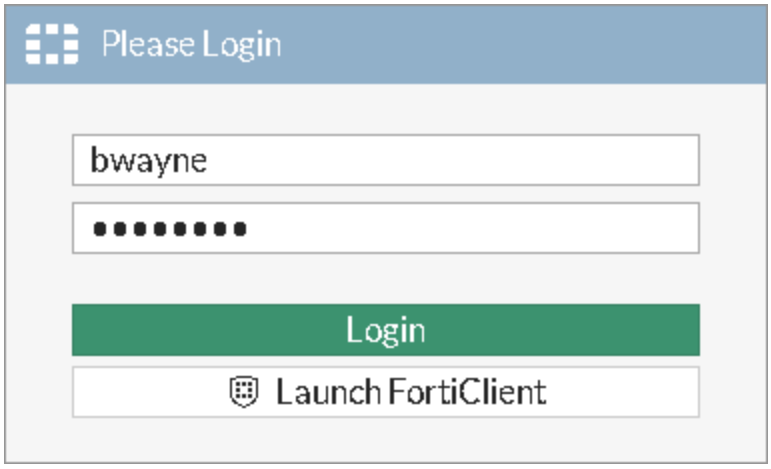


4. Select the prompt at the top of the screen to create a new SSL-VPN policy, including the *LDAPgroup*, as shown.

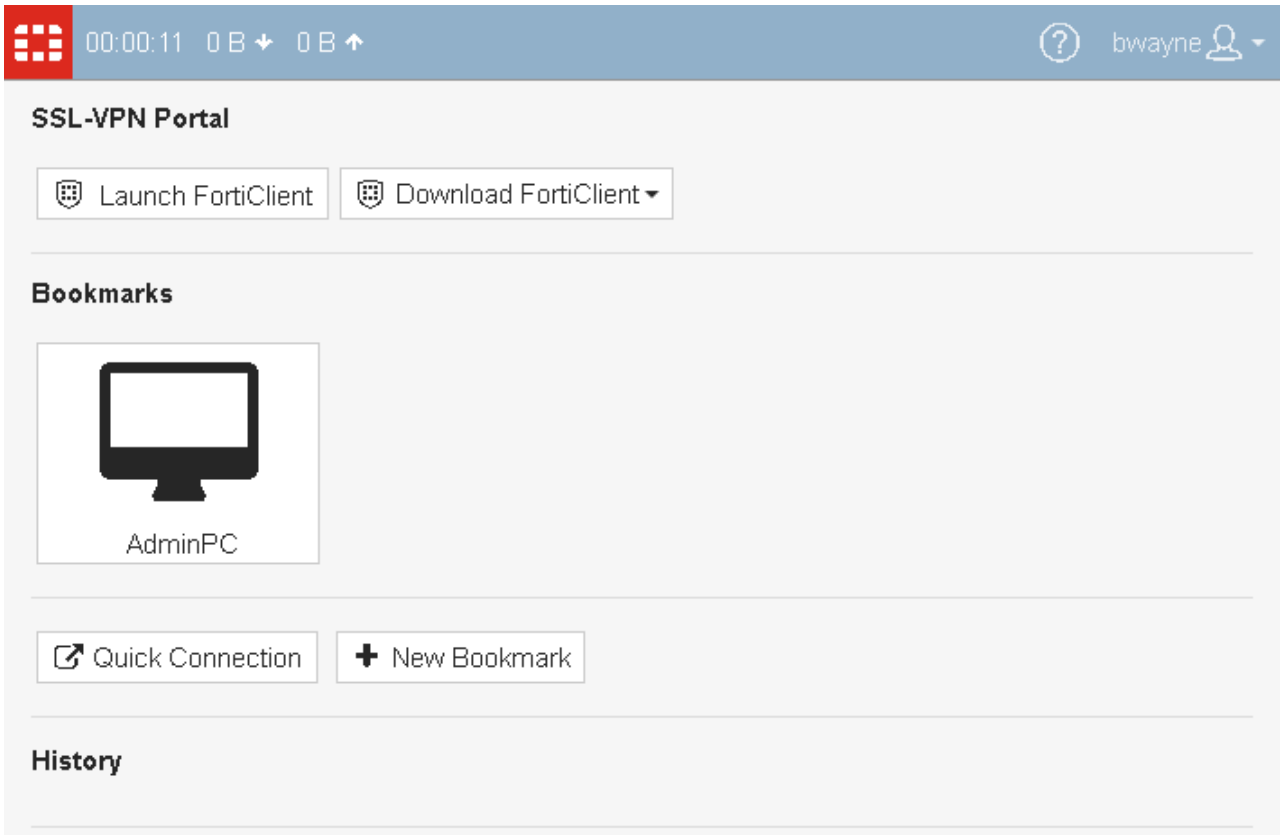


Results

1. From a remote device, access the SSL VPN Web Portal.
   Enter valid LDAP credentials (in the example, bwayne).



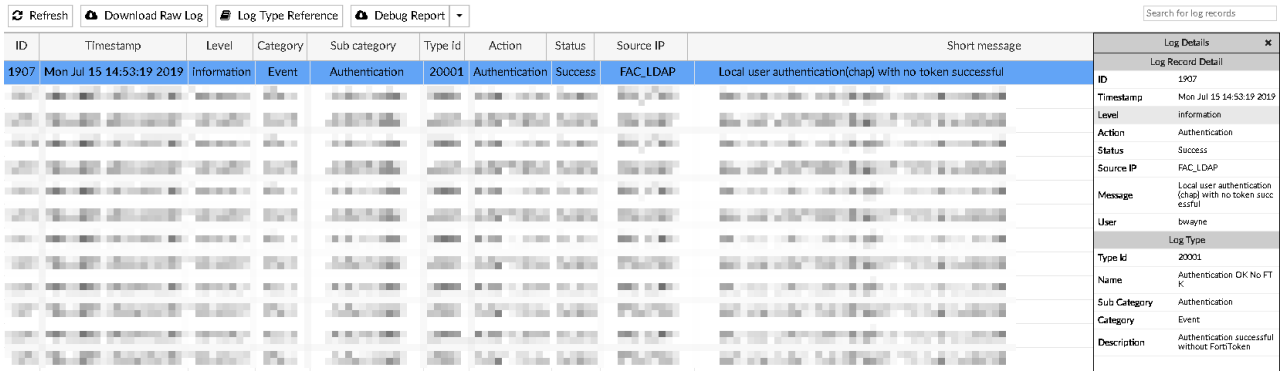
2. The user is now successfully logged into the SSL VPN Portal.



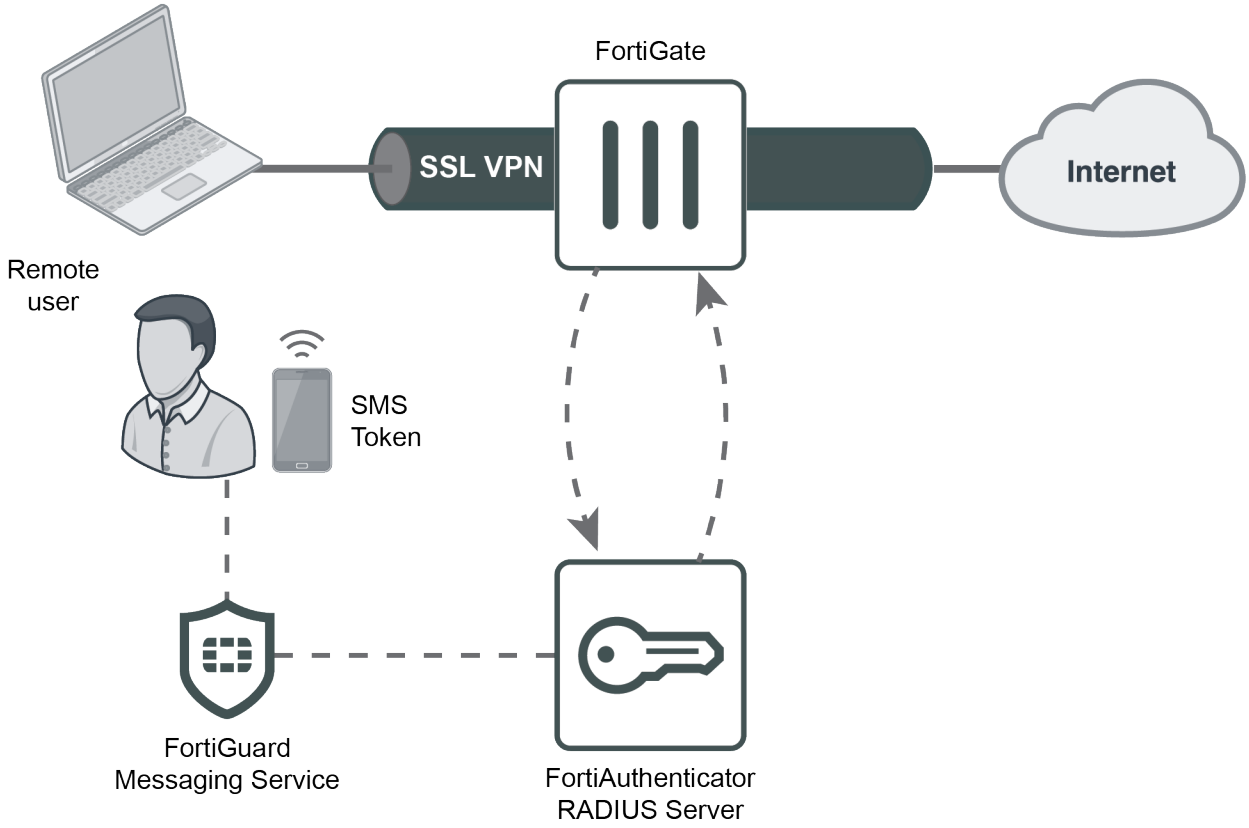
3. On the FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the connection.

Username	Last Login	Remote Host	Active Connections
bwayne	2019/07/15 11:53:19	172.25.181.138	

4. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* and confirm the connection.



SMS two-factor authentication for SSL VPN



In this recipe, you will create an SSL VPN with two-factor authentication consisting of a username, password, and an SMS token.

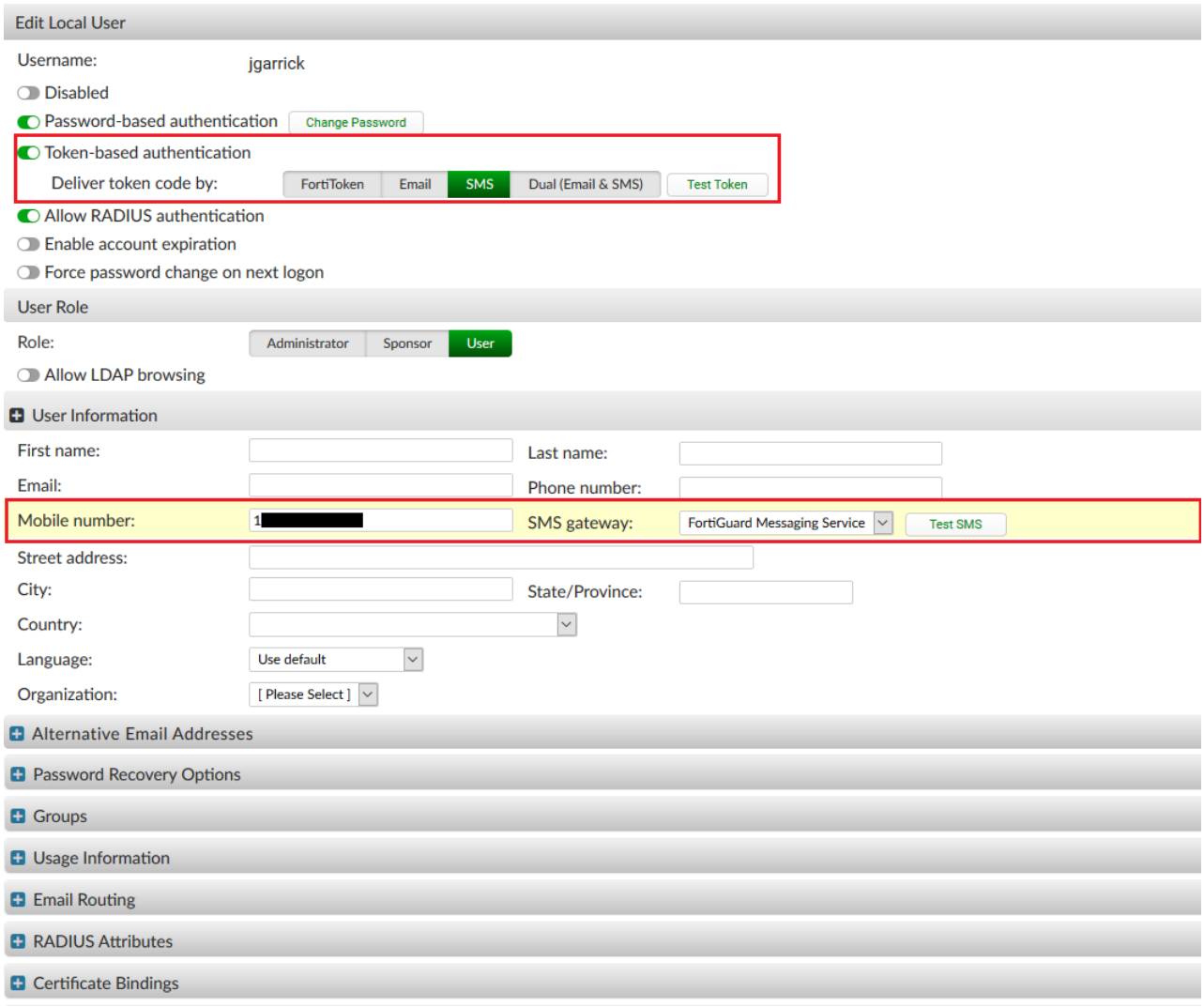
When a user attempts to connect to this SSL VPN, they are prompted to enter their username and password. After successfully entering their credentials, they receive an SMS message on their mobile phone containing a 6-digit number (called the FortiToken code). They must also enter this number to get access to the internal network and the Internet.

Although this recipe uses the FortiGuard Messaging Service, it will also work with any compatible SMS service you configure as an SMS Gateway.

Creating an SMS user and user group on the FortiAuthenticator

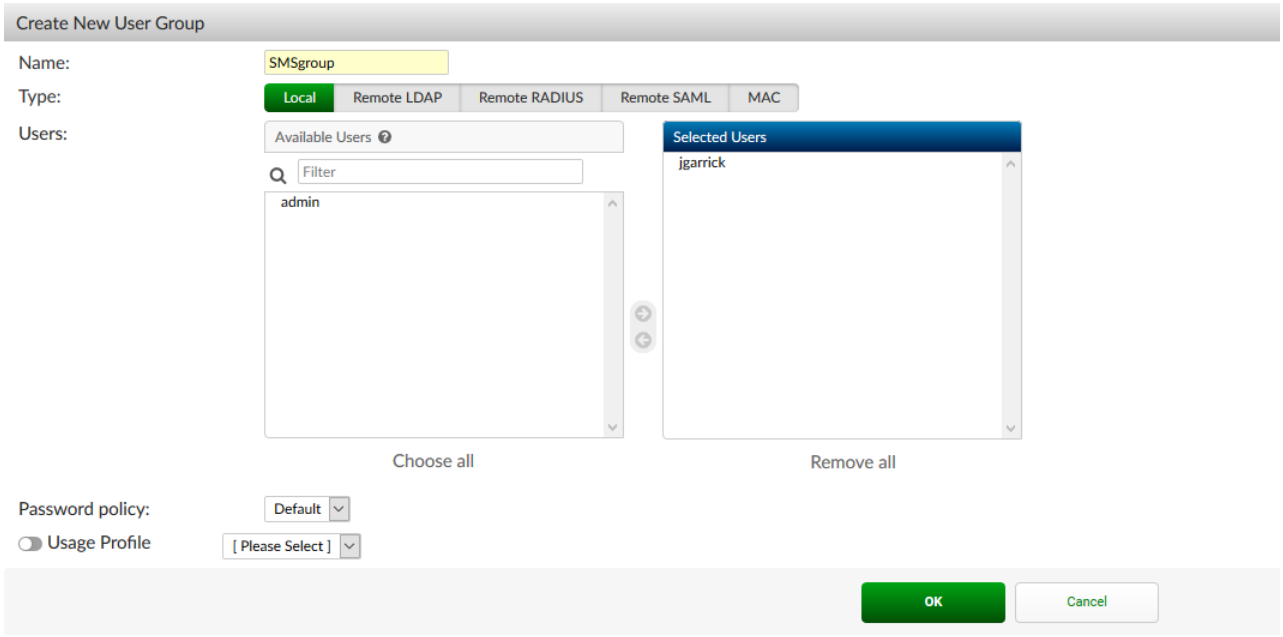
To create an SMS user and user group:

1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and add/modify a user to include *SMS Token-based authentication* and a *Mobile number* using the preferred *SMS gateway* as shown.
   The *Mobile number* must be in the following format:
   `+[international-number]`
   Enable *Allow RADIUS authentication*.



2. Go to *Authentication* > *User Management* > *User Groups* and add the above user to a new SMS user group (in the

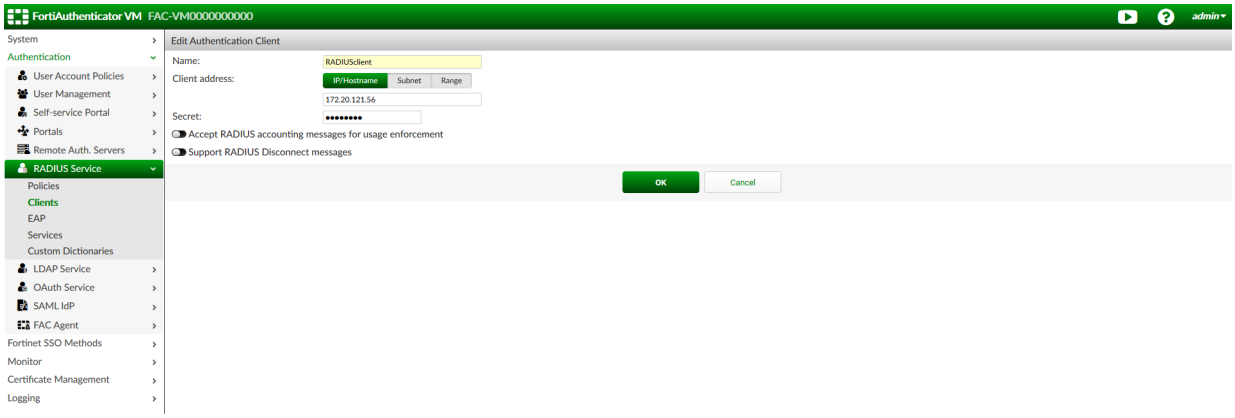
example, *SMSgroup*).



Configuring the FortiAuthenticator RADIUS client

To create the RADIUS client:

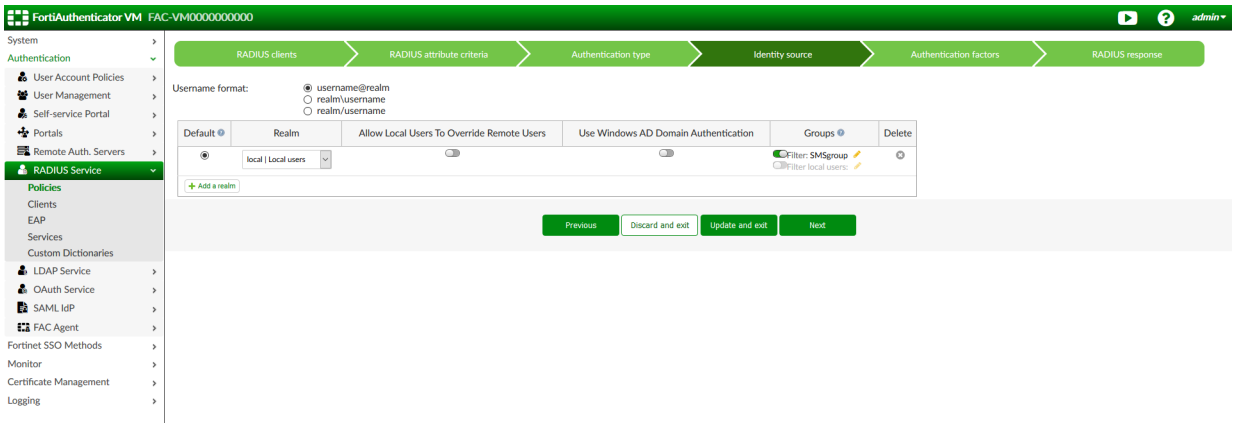
1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.
3. Click *OK*.



To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Optionally, configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type.

5. Choose a username format (in this example: *username@realm*), select the *Local* realm, and add the *SMSgroup* as a filter.

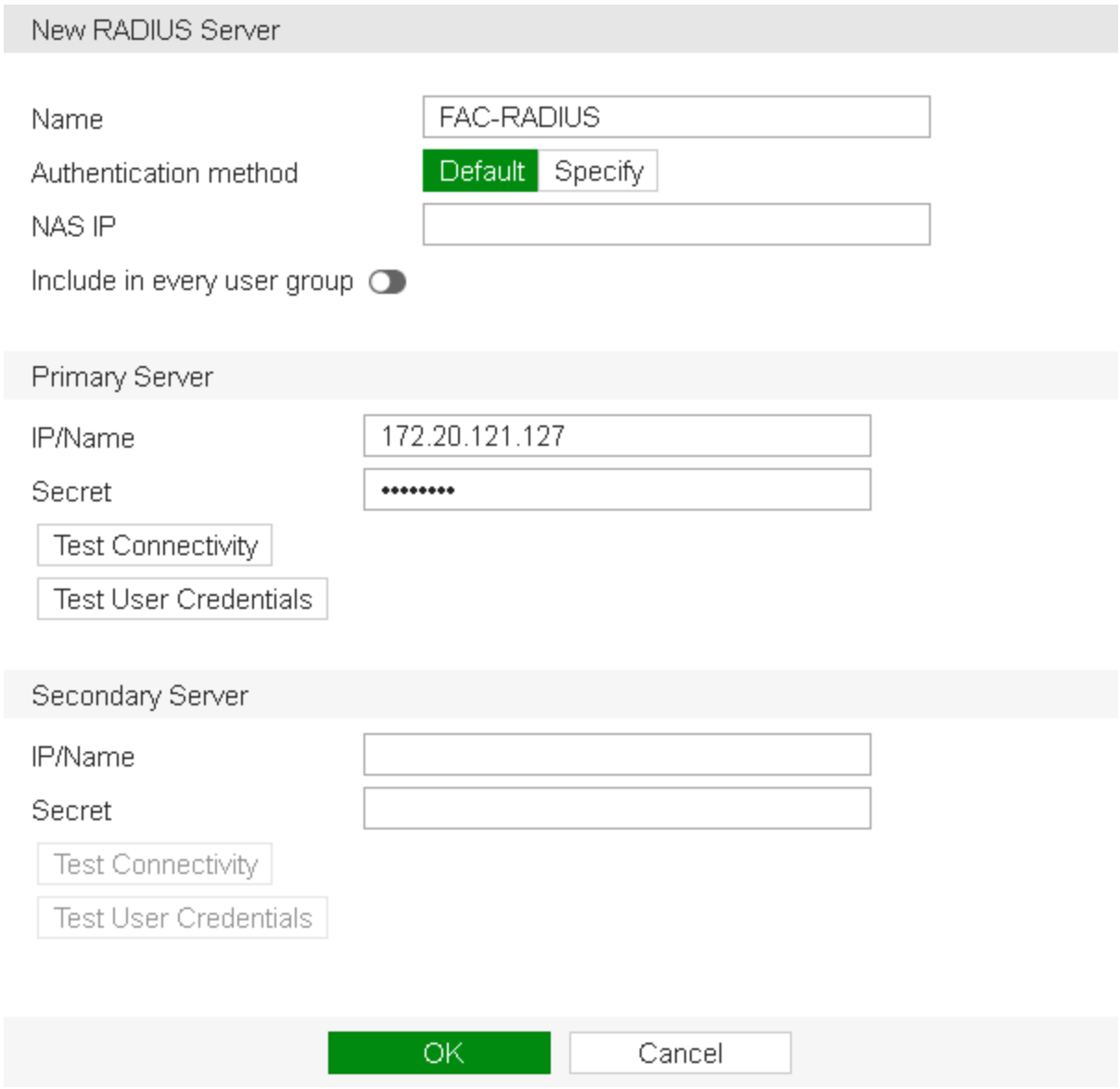


6. Set the authentication method to *Mandatory two-factor authentication*.
7. Click *Save and Exit*.

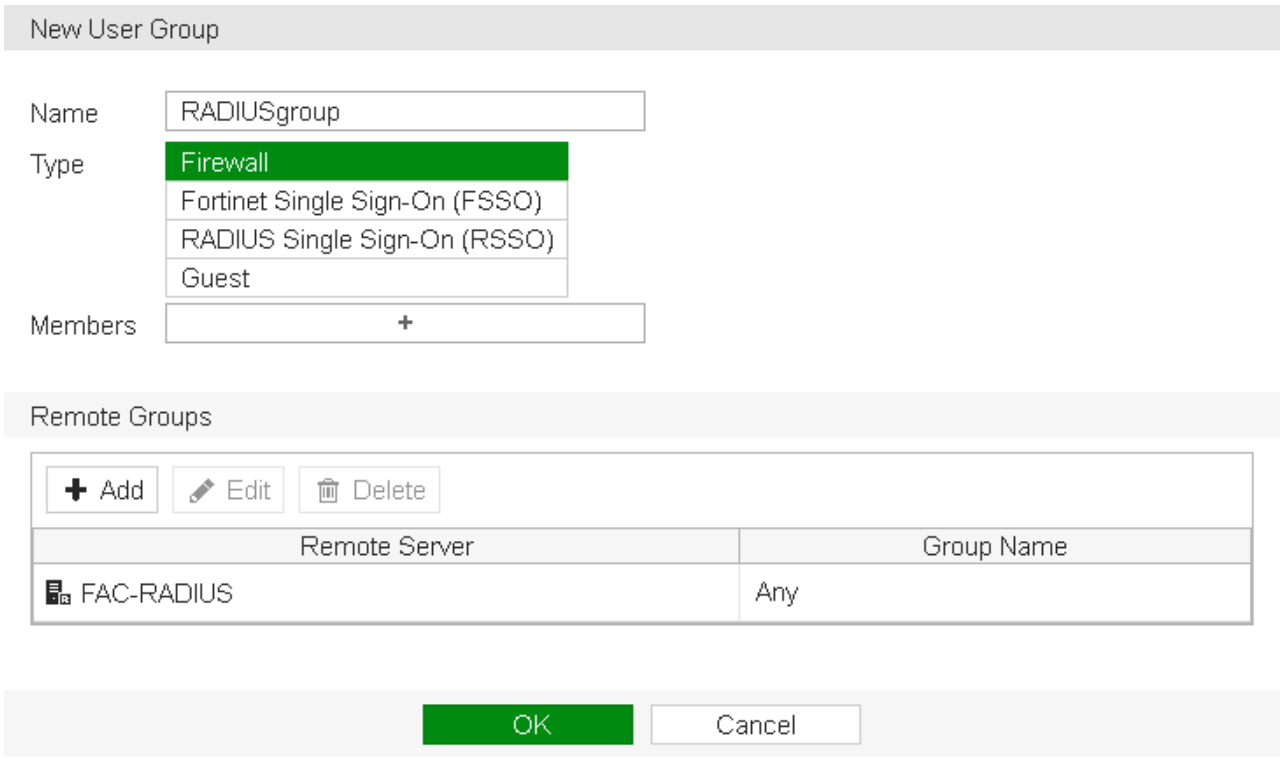
Configuring the FortiGate authentication settings

To configure the FortiGate authentication settings:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and create the connection to the FortiAuthenticator RADIUS server, using its IP address and pre-shared secret.
   Use *Test Connectivity* to make sure that the FortiGate can communicate with the FortiAuthenticator.



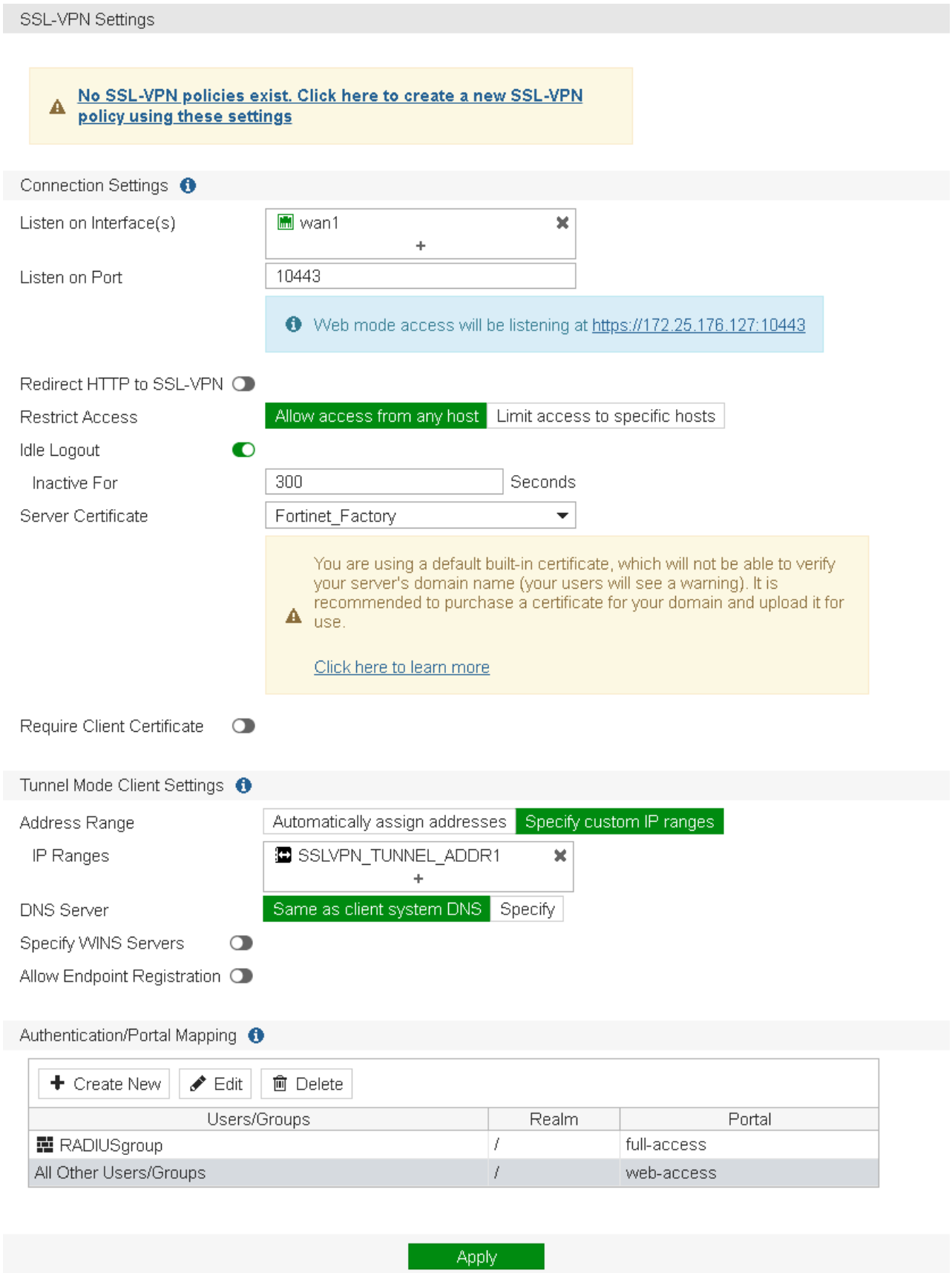
2. Next, go to *User & Device* > *User Groups* and create a RADIUS user group called *RADIUSgroup*. Set the *Type* to *Firewall* and add the RADIUS server to the *Remote groups* table.



Configuring the SSL-VPN

Configure the SSL-VPN settings:

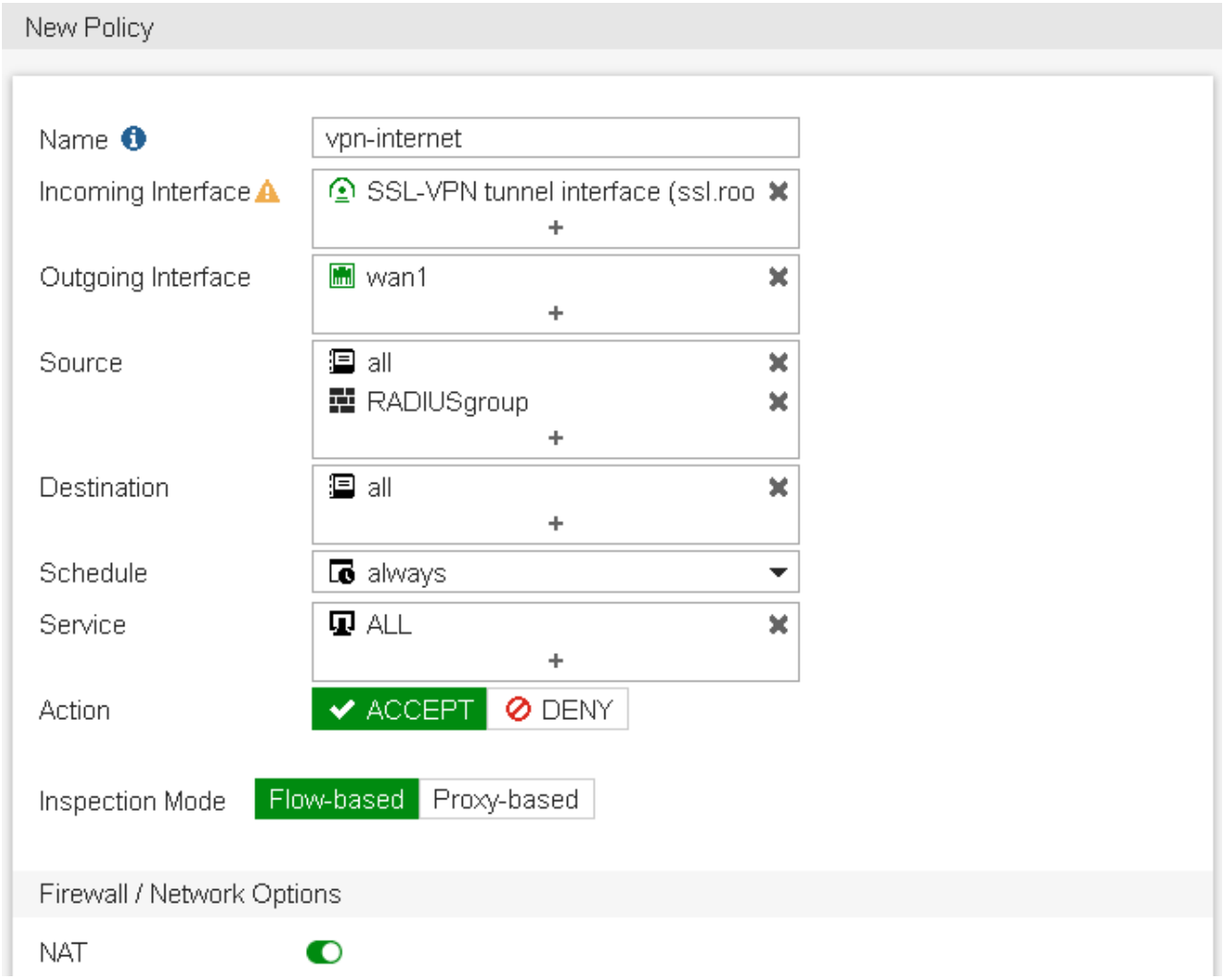
1. Go to *VPN* > *SSL-VPN Settings*.
   Under *Connection Settings*, set *Listen on Port* to `10443`. Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set *IP Ranges* to the SSL VPN tunnel address range.
   Under *Authentication/Portal Mapping*, select *Create New*.
   Assign the *RADIUSgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal.


SSL-VPN Settings
No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.127:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
IP Ranges
SSLVPN_TUNNEL_ADDR1
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
Portal
RADIUSgroup
/
full-access
All Other Users/Groups
/
web-access
Apply

Creating the security policy for VPN access to the Internet

To create the security profile:

1. Go to *Policy & Objects* > *IPv4 Policy* and create a new SSL-VPN policy, including the *RADIUSgroup*, as shown.

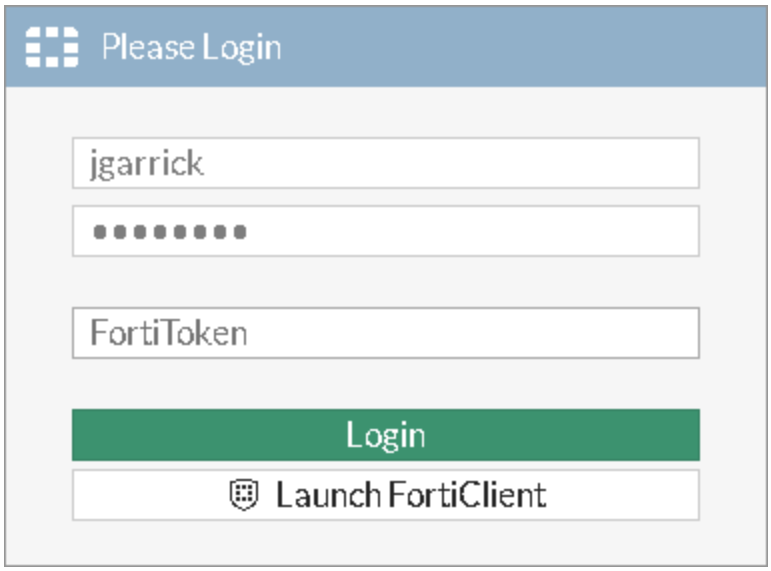


Results

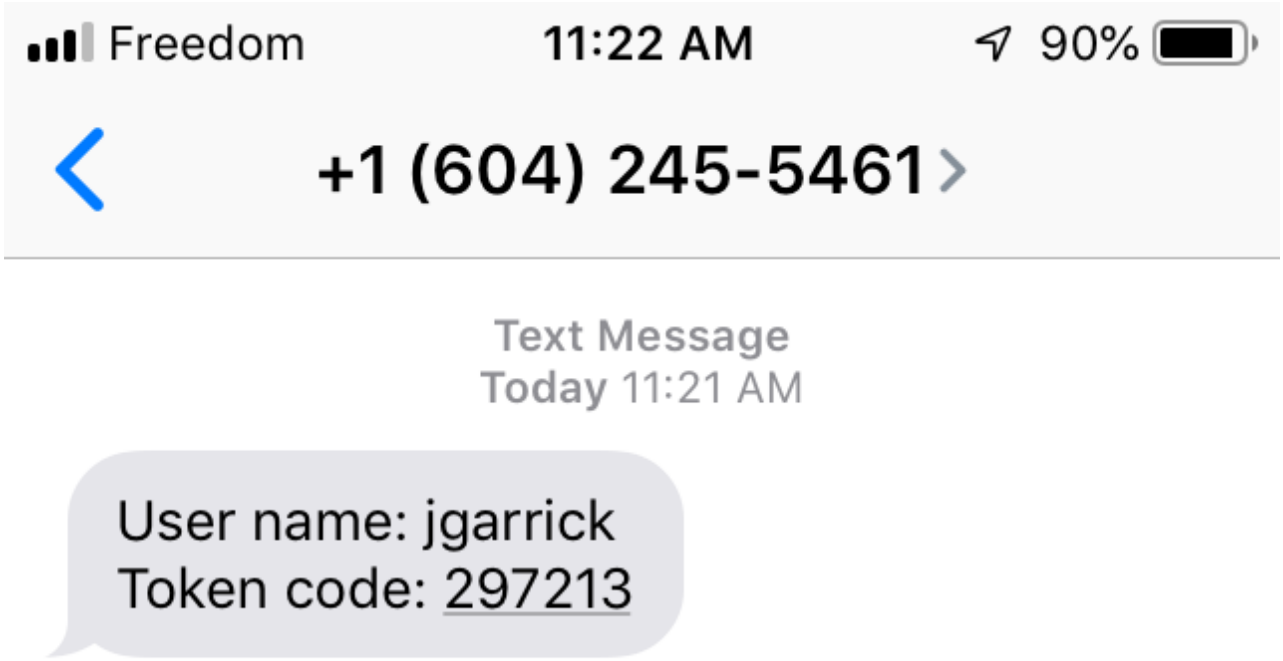
In this example, we will use the web portal to access the SSL VPN and test the two-factor authentication.

To test two-factor authentication:

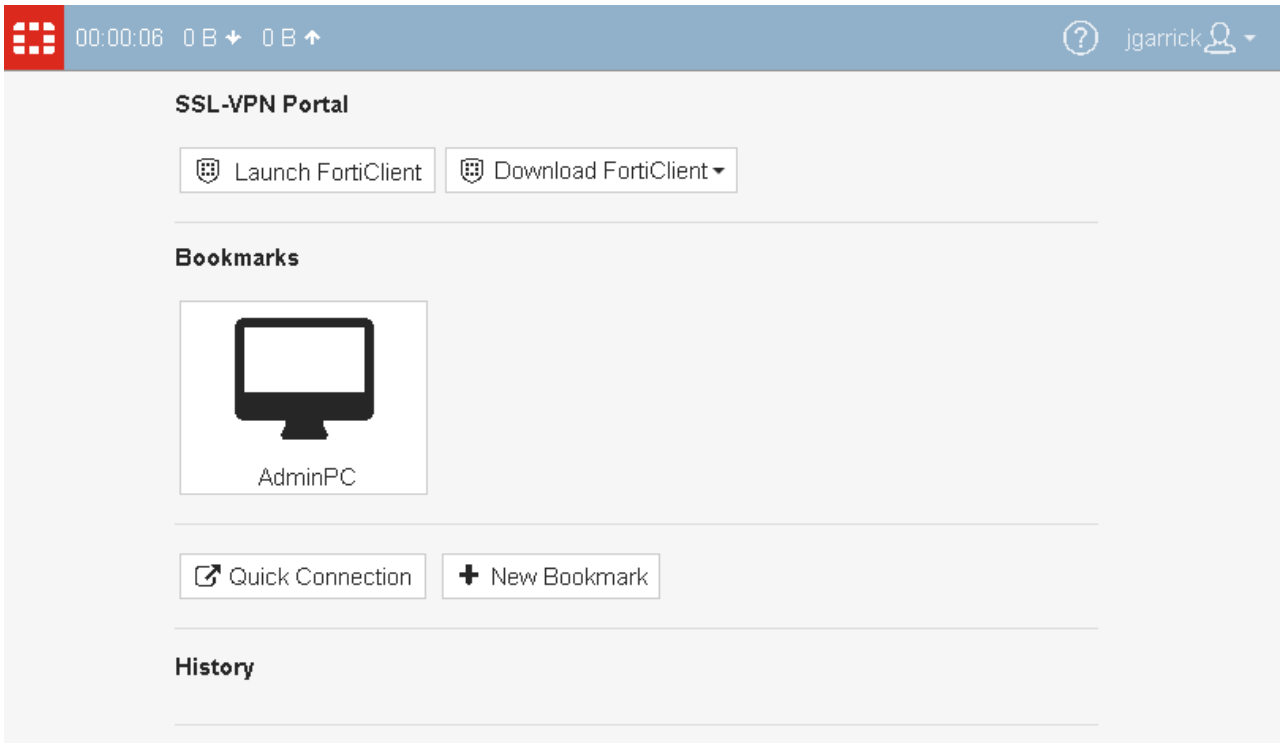
1. Open a browser and navigate to the SSL VPN web portal, in this case *https://172.25.176.127:10443*.
   Enter a valid username and password and select *Login*. You should be prompted to enter a *FortiToken Code*.



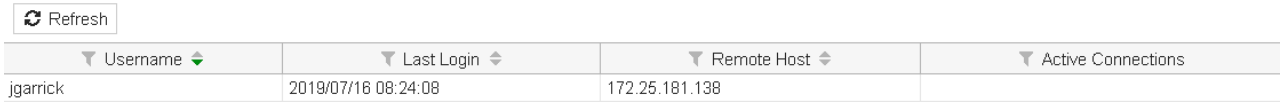
2. The *FortiToken Code* should have been sent to your mobile phone as a text message containing a 6-digit number. Enter the number into the SSL VPN login portal and select *Login*.


Freedom
11:22 AM
90%
+1 (604) 245-5461
Text Message
Today 11:21 AM
User name: jgarrick
Token code: 297213

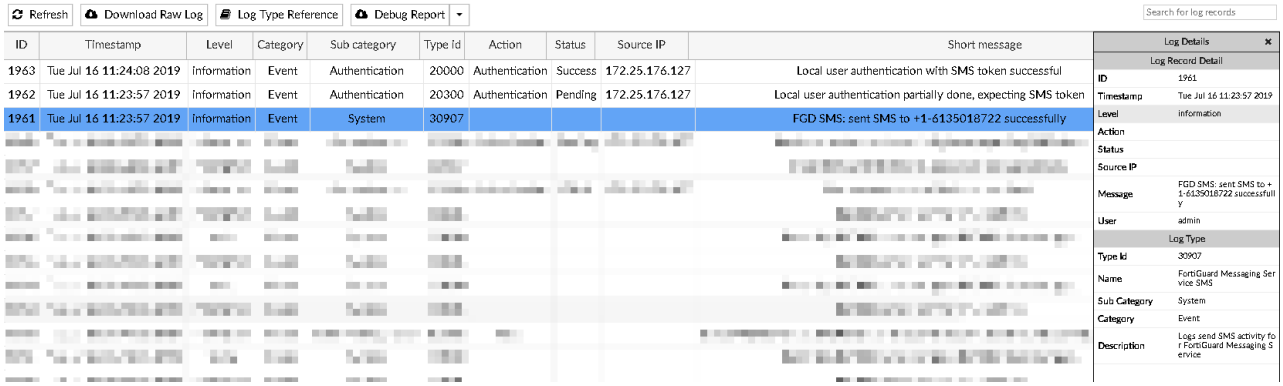
3. You should now have access to the SSL VPN tunnel.



4. To verify that the user has connected to the tunnel, on the FortiGate, go to *Monitor* > *SSL-VPN Monitor*.



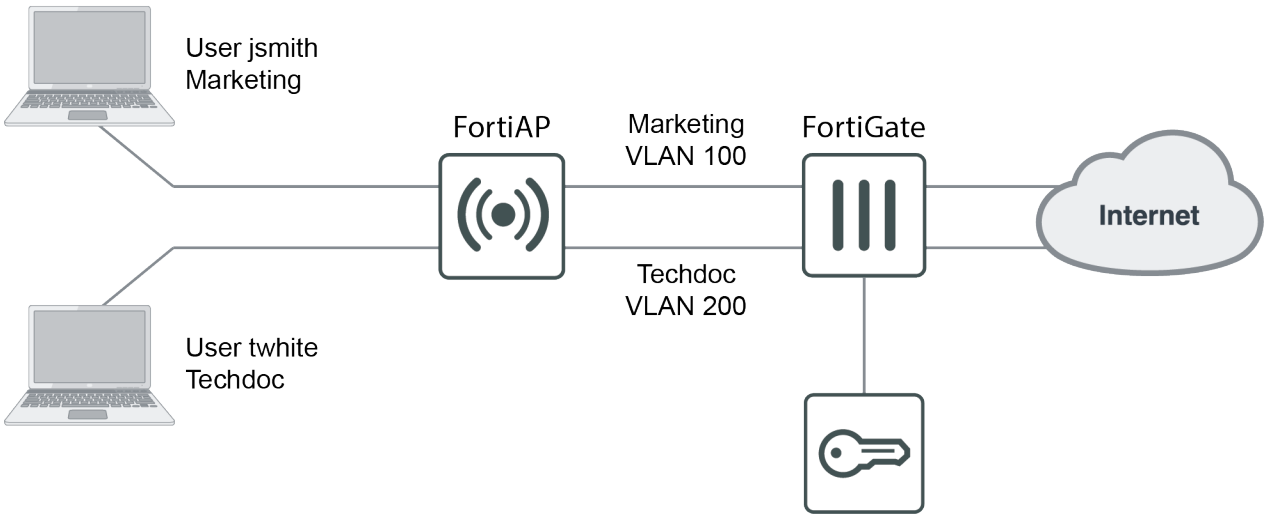
5. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the user's connection.



WiFi authentication

This section describes configuring WiFi authentication with FortiAuthenticator.

Assigning WiFi users to VLANs dynamically



Virtual LANs (VLANs) are used to assign wireless users to different networks without requiring the use of multiple SSIDs. Each user's VLAN assignment is stored in the user database of the RADIUS server that authenticates the users.

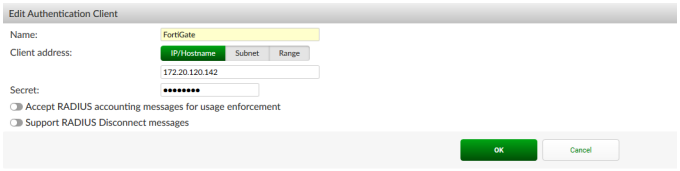
This example creates dynamic VLANs for the Techdoc and Marketing departments. The RADIUS server is a FortiAuthenticator. It is assumed a user group on the FortiAuthenticator has already been created (in this example, *employees*).

```
config certificate ca
    edit {name}
    # CA certificate.
        set name {string}   Name. size[79]
        set ca {string}   CA certificate as a PEM file.
        set range {global | vdom}   Either global or VDOM IP address range for the CA cer-
tificate.
                global  Global range.
                vdom    VDOM IP address range.
        set source {factory | user | bundle}   CA certificate source type.
                factory  Factory installed certificate.
                user     User generated certificate.
                bundle   Bundle file certificate.
        set trusted {enable | disable}   Enable/disable as a trusted CA.
        set scep-url {string}   URL of the SCEP server. size[255]
        set auto-update-days {integer}   Number of days to wait before requesting an updated
CA certificate (0 - 4294967295, 0 = disabled). range[0-4294967295]
```

Configuring the FortiAuthenticator

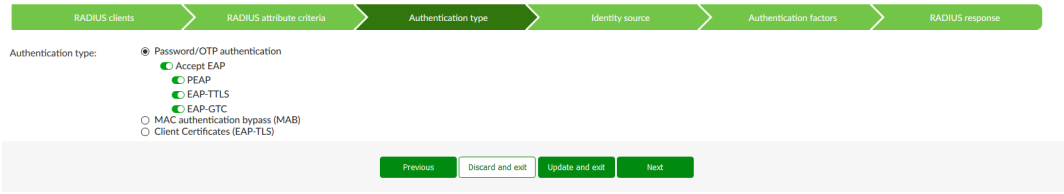
To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.



To create the RADIUS policy:

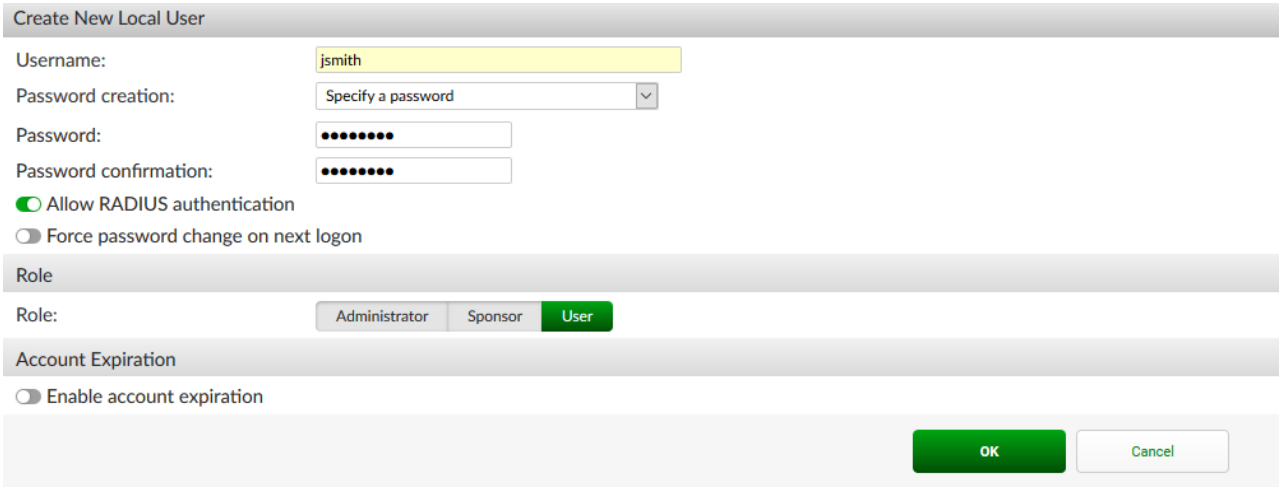
1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type and enable all *EAP* types.



5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
   Add the *employees* user group as a filter.
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

To create the local user accounts:

1. Next go to *Authentication* > *User Management* > *Local Users* and create local user accounts as needed.



2. For each user, add the following RADIUS attributes which specify the VLAN information to be sent to the FortiGate.

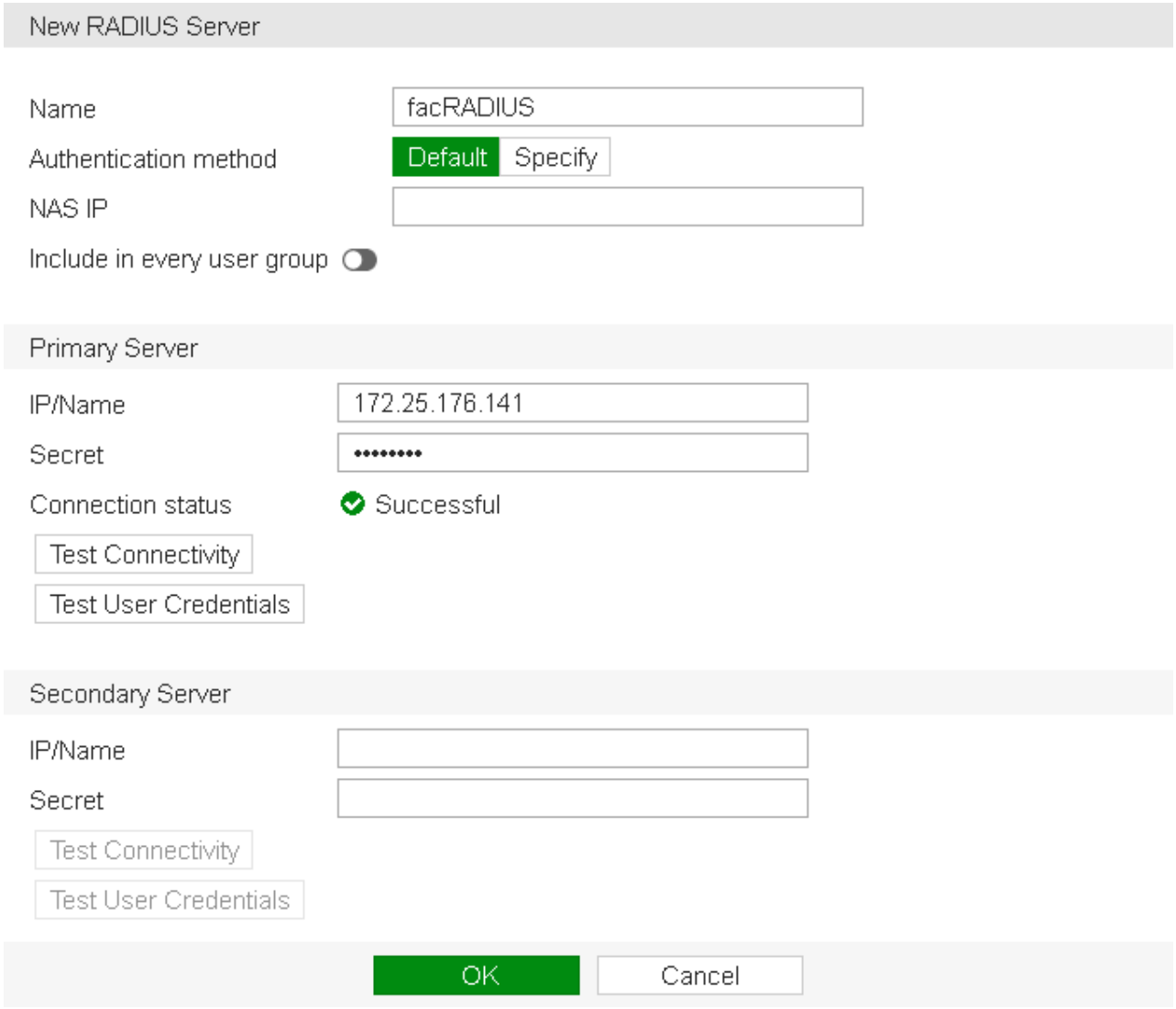
The *Tunnel-Private-Group-Id* attribute specifies the VLAN ID.

In this example, jsmith is assigned VLAN *100* and twhite is assigned VLAN *200*.

Adding the RADIUS server to the FortiGate

To add the RADIUS server to the FortiGate:

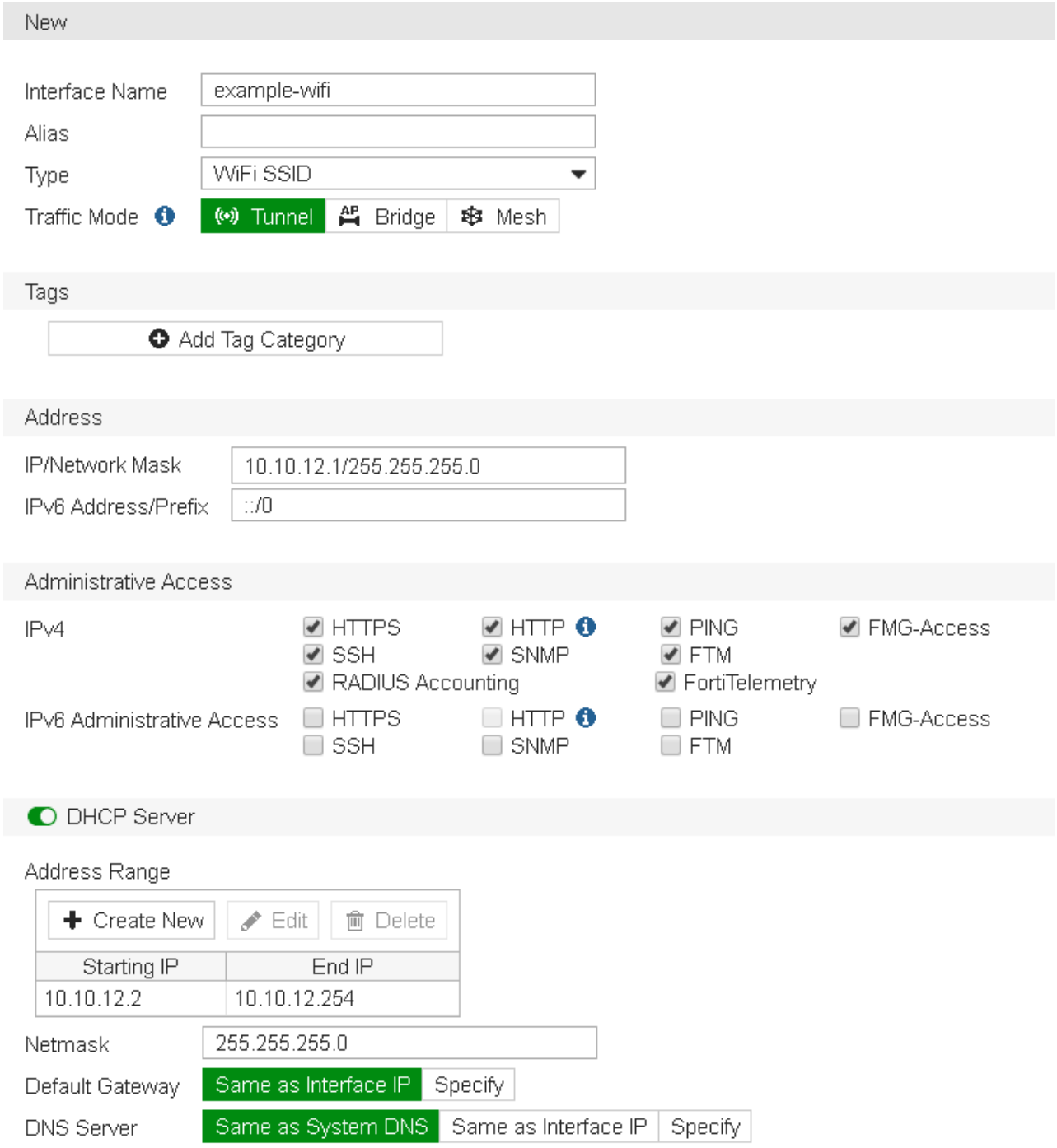
1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*.
   Enter the FortiAuthenticator IP address and the server *Secret* entered on the FortiAuthenticator earlier.
   Select *Test Connectivity* to confirm the successful connection.



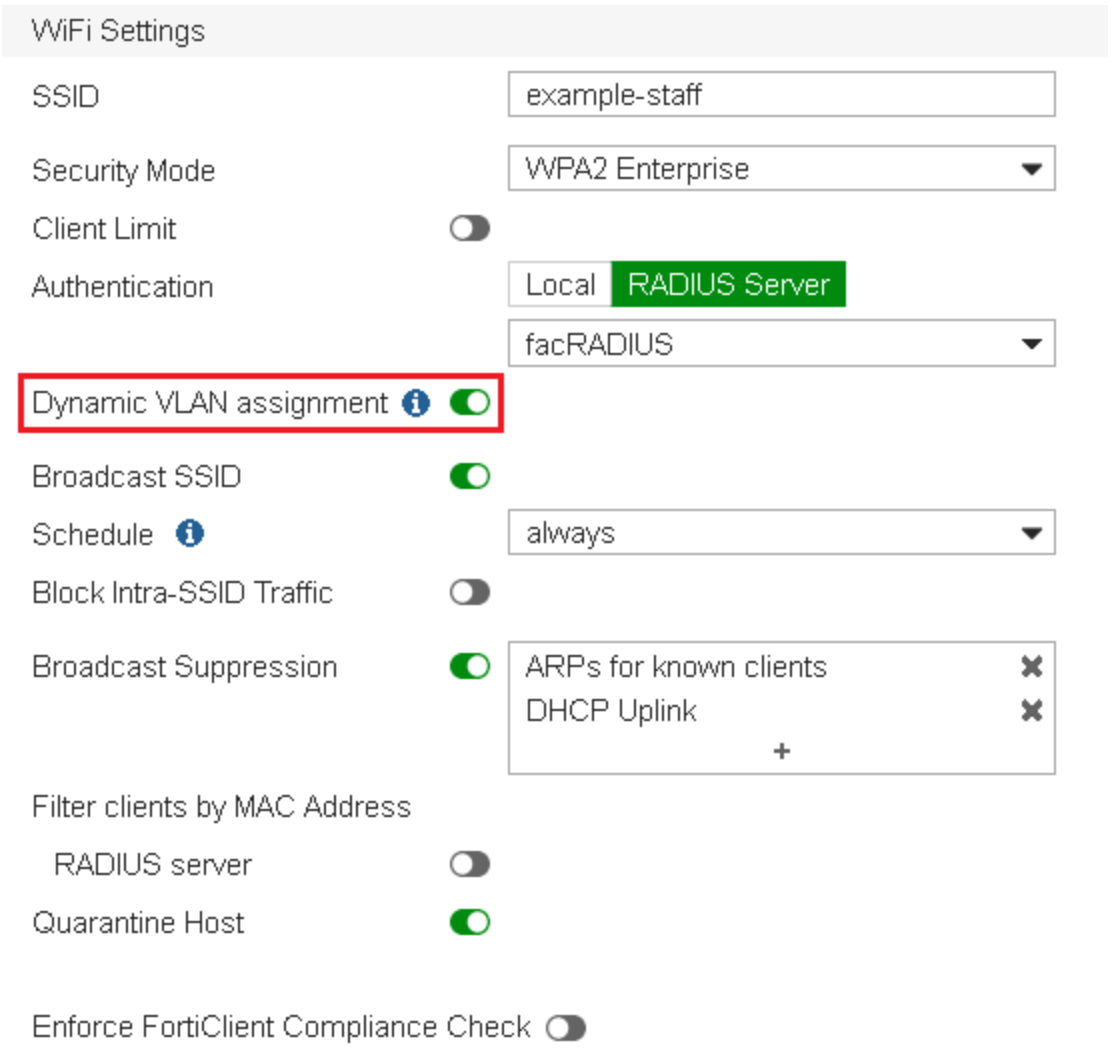
Creating an SSID with dynamic VLAN assignment

To create an SSID with dynamic VLAN assignment:

1. On the FortiGate, go to *WiFi & Switch Controller* > *SSID* and create a new SSID.
   Set up DHCP service.



2. Select *WPA2 Enterprise* security and select your RADIUS server for authentication.
   Enable *Dynamic VLAN Assignment*.



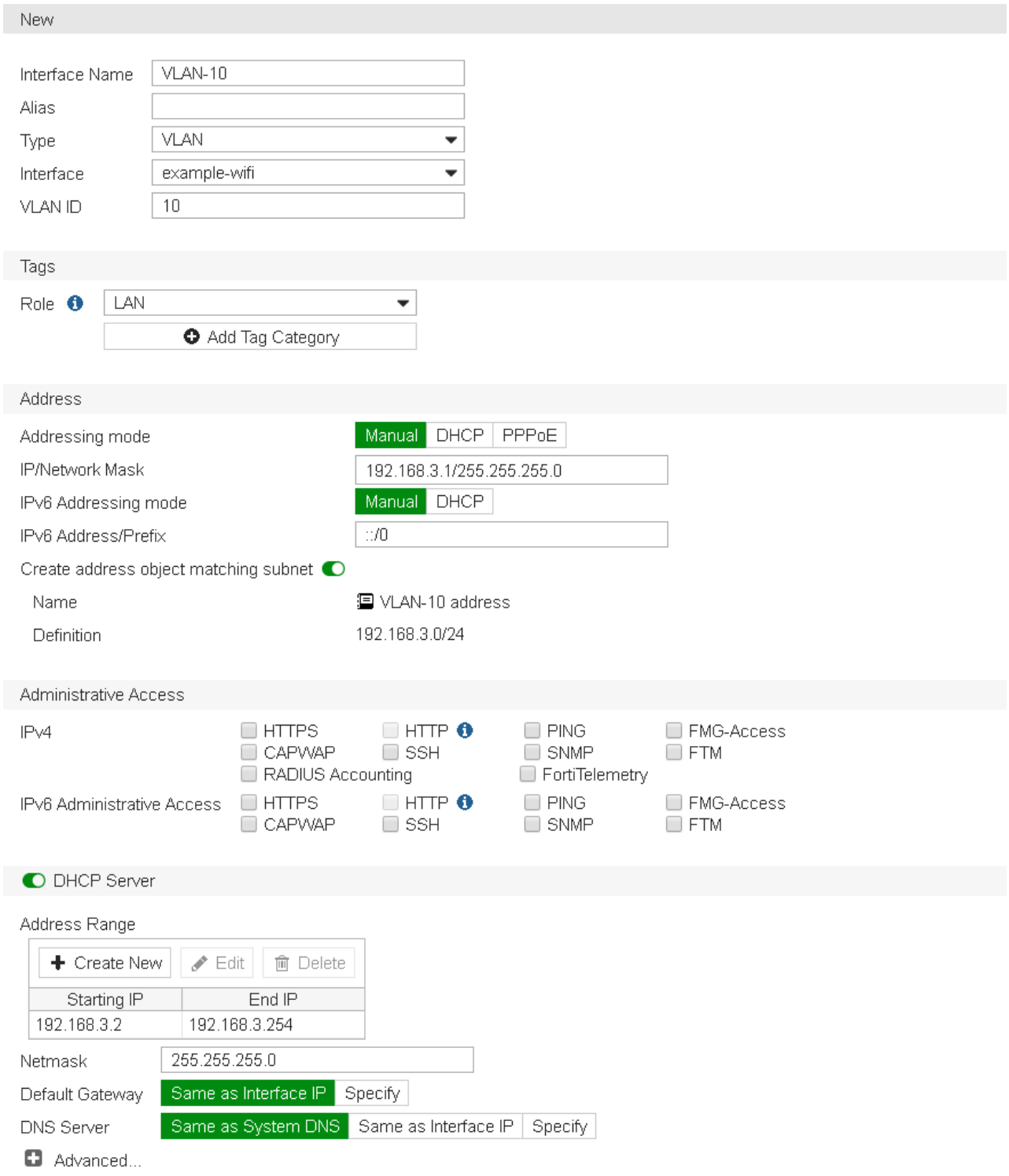
3. Then open the *CLI Console* and enter the following command to assignment and set the VLAN ID to `10`. This VLAN is used when RADIUS does not assign a VLAN:

```
config wireless-controller vap
   edit example-wifi
      set vlanid 10
   next
end
```

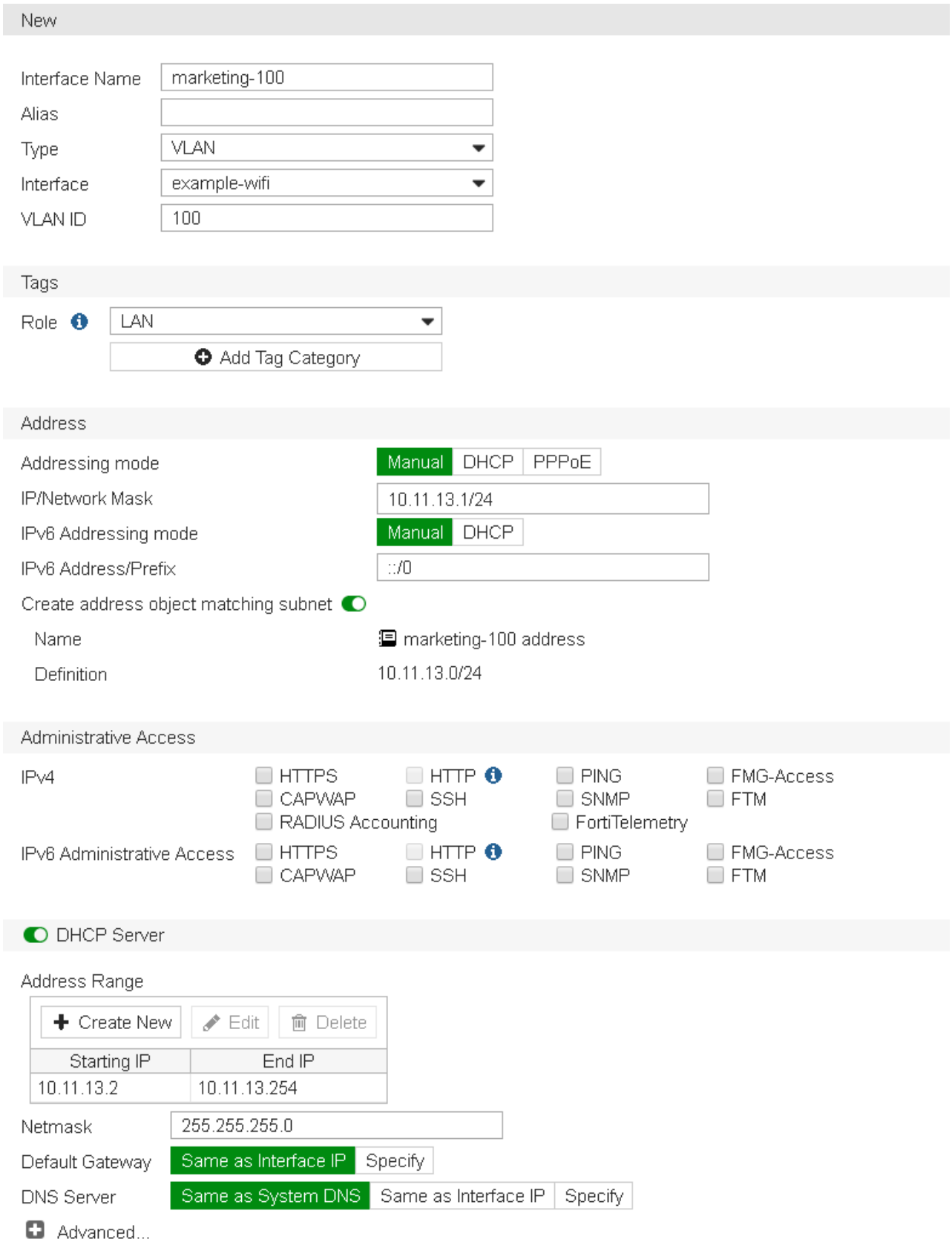
Creating the VLAN interfaces

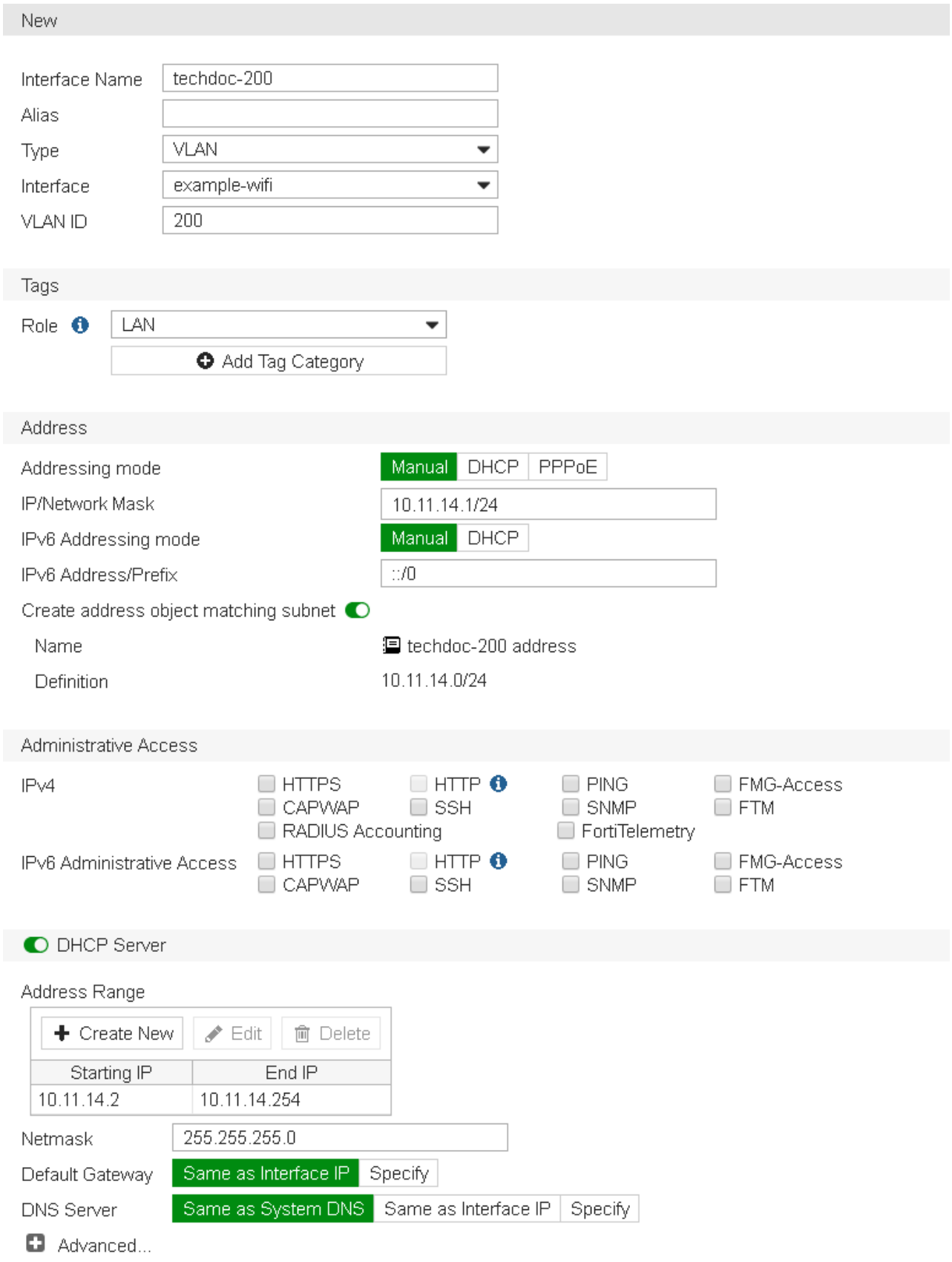
To create the VLAN interfaces:

1. Go to *Network* > *Interfaces*.
   Create the VLAN interface for default *VLAN-10* and set up DHCP service.



2. Then create two more VLAN interfaces: one for *marketing-100* and another for *techdoc-200*, both with DHCP service.

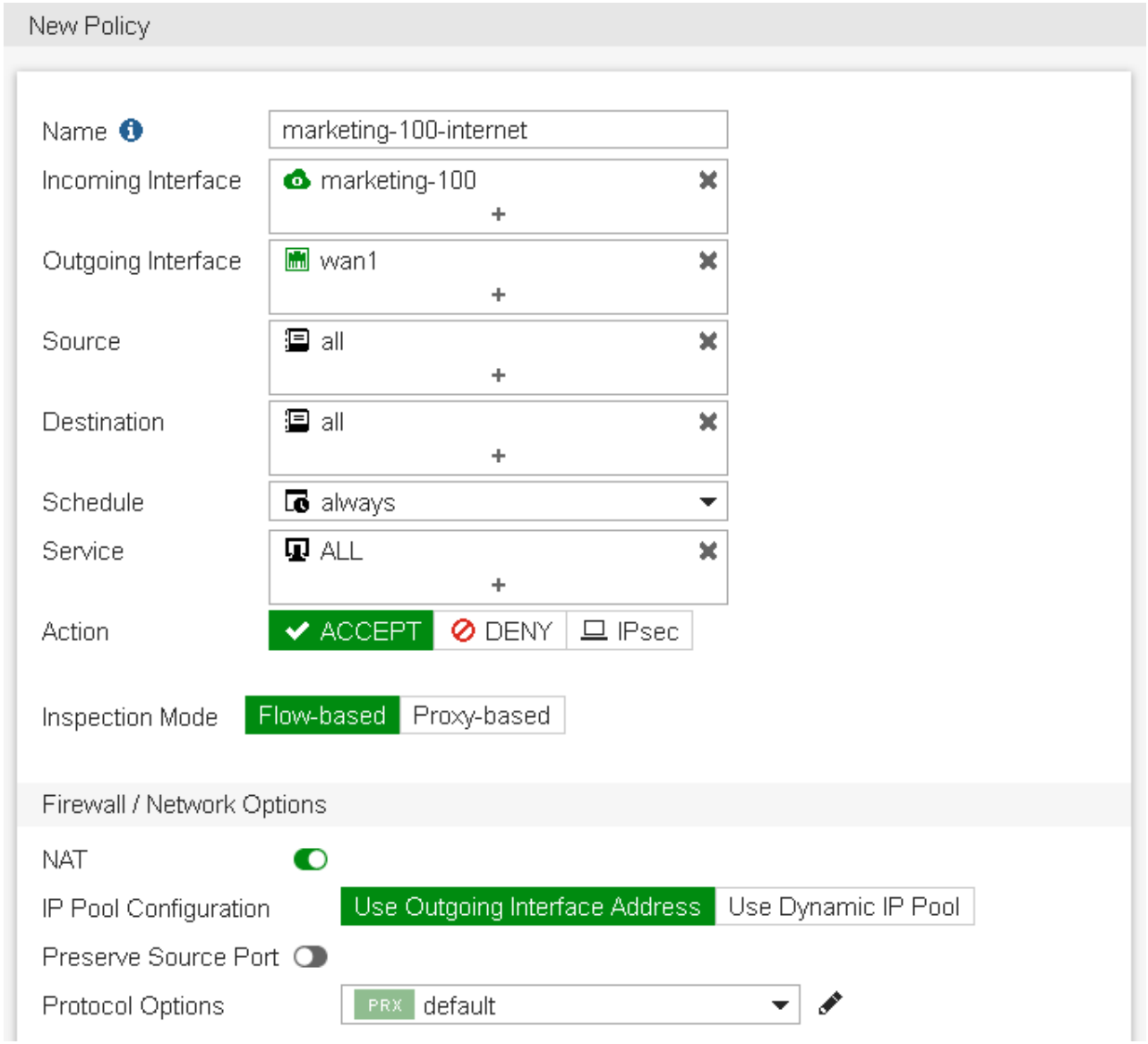

New
Interface Name
marketing-100
Alias
Type
VLAN
Interface
example-wifi
VLAN ID
100
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
10.11.13.1/24
IPv6 Addressing mode
Manual
DHCP
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
marketing-100 address
Definition
10.11.13.0/24
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
IPv6 Administrative Access
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
DHCP Server
Address Range
Create New
Edit
Delete
Starting IP
End IP
10.11.13.2
10.11.13.254
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Same as Interface IP
Specify
Advanced...


New
Interface Name
techdoc-200
Alias
Type
VLAN
Interface
example-wifi
VLAN ID
200
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
10.11.14.1/24
IPv6 Addressing mode
Manual
DHCP
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
techdoc-200 address
Definition
10.11.14.0/24
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
IPv6 Administrative Access
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
DHCP Server
Address Range
Create New
Edit
Delete
Starting IP
End IP
10.11.14.2
10.11.14.254
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Same as Interface IP
Specify
Advanced...

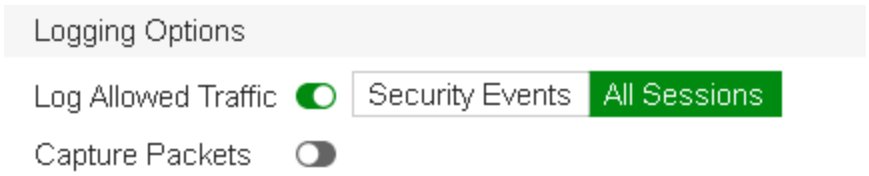
Creating security policies

To create the security policies:

1. Go to *Policy & Objects* > *IPv4 Policy*.
   Create a policy that allows outbound traffic from *marketing-100* to the Internet.

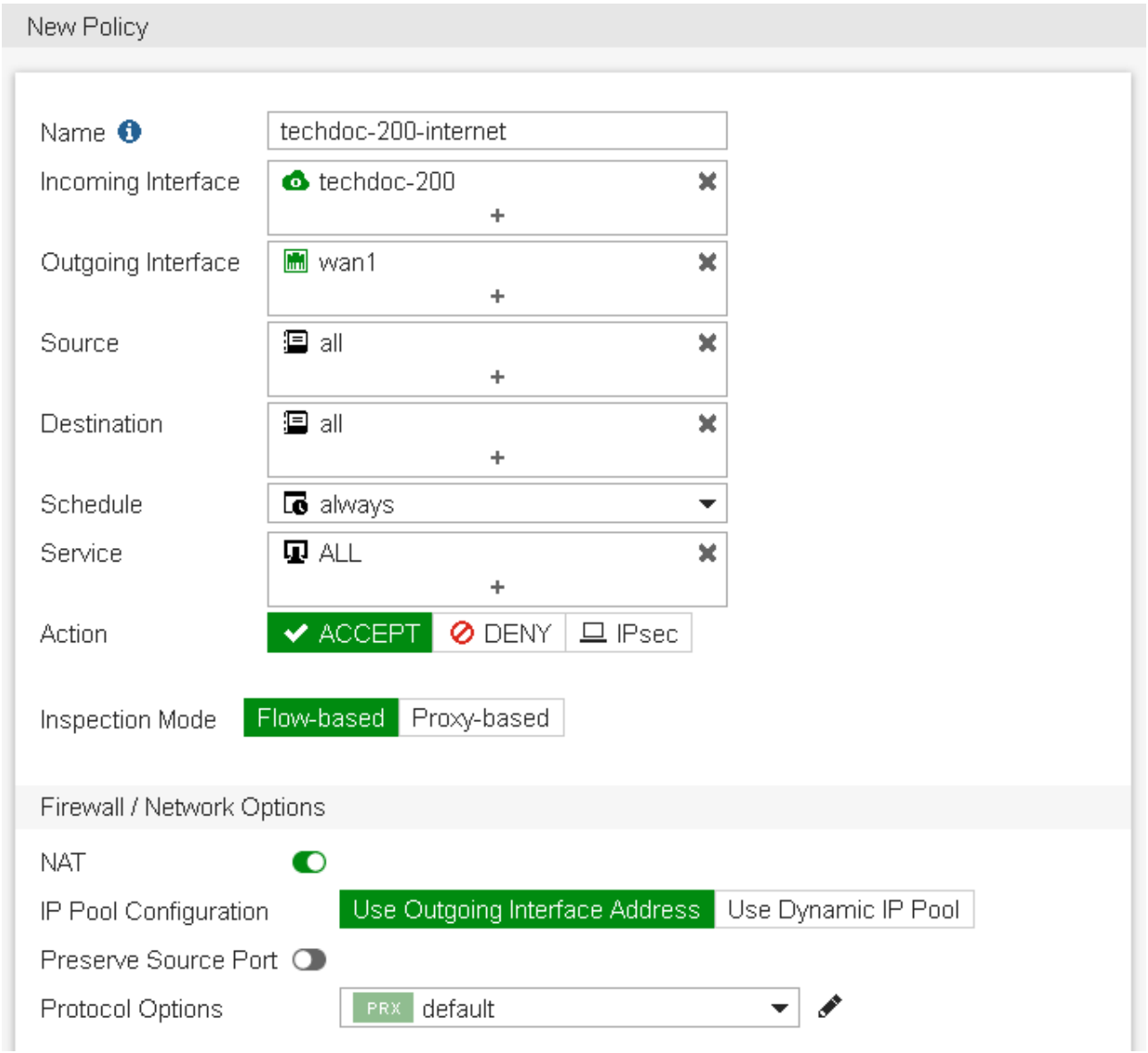


2. Under *Logging Options*, enable logging for *All Sessions*.



3. Create another policy that allows outbound traffic from *techdoc-200* to the Internet.

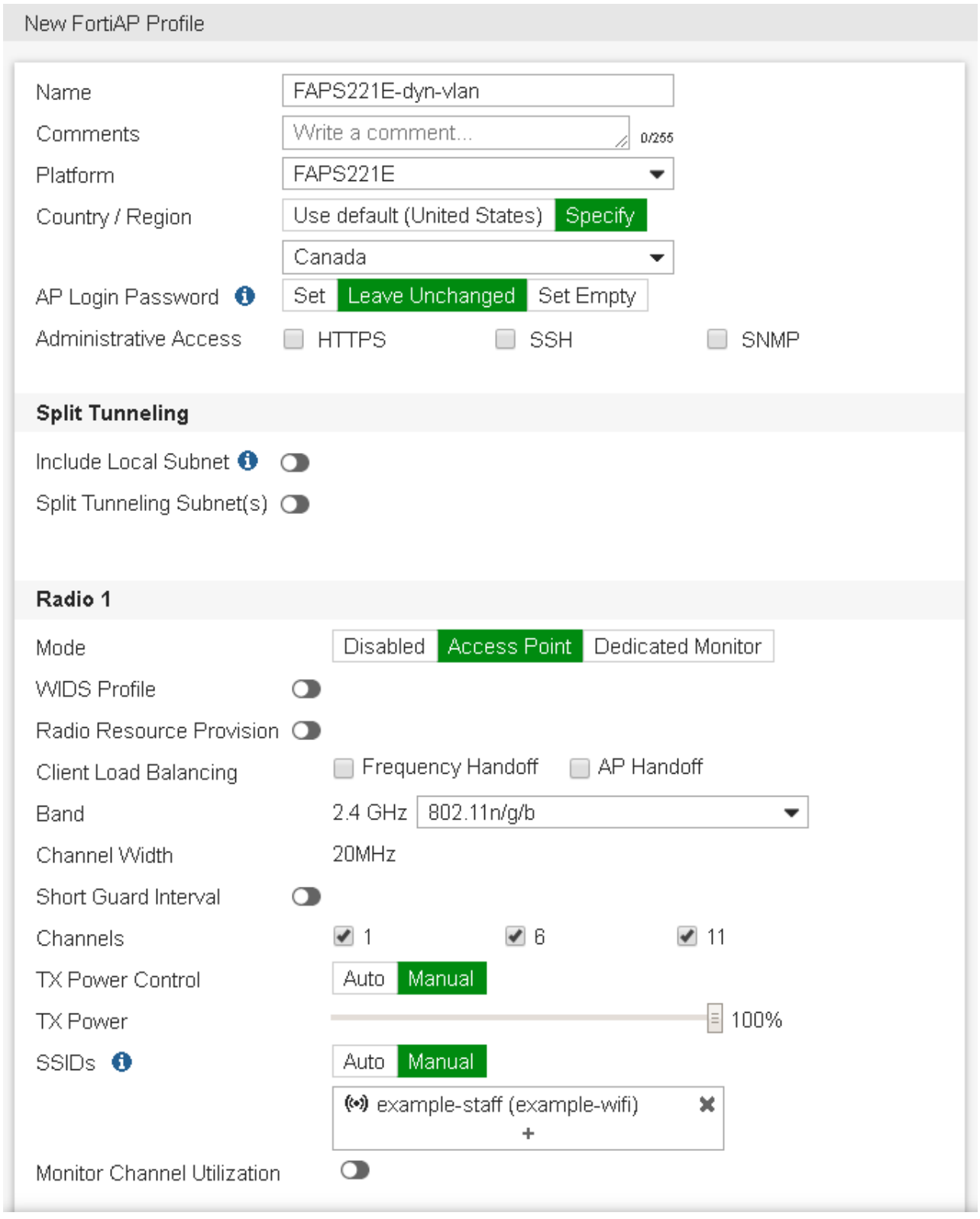
For this policy too, under *Logging Options*, enable logging for *All Sessions*.



Creating the FortiAP profile

To create the FortiAP profile:

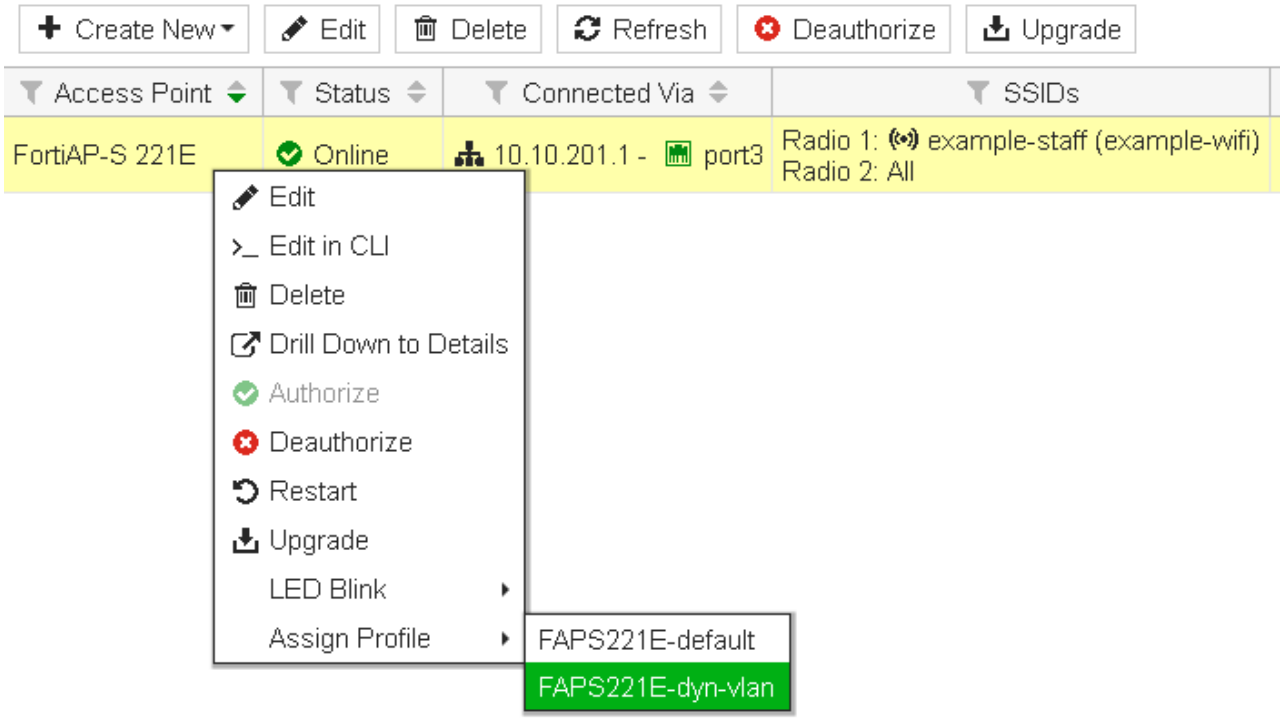
1. Go to *WiFi & Switch Controller* > *FortiAP Profiles*.
   Create a new profile for your FortiAP model and select the new SSID for both *Radio 1* and *Radio 2*.


New FortiAP Profile
Name
FAPS221E-dyn-vlan
Comments
Write a comment...
0/255
Platform
FAPS221E
Country / Region
Use default (United States)
Specify
Canada
AP Login Password
Set
Leave Unchanged
Set Empty
Administrative Access
HTTPS
SSH
SNMP
Split Tunneling
Include Local Subnet
Split Tunneling Subnet(s)
Radio 1
Mode
Disabled
Access Point
Dedicated Monitor
WIDS Profile
Radio Resource Provision
Client Load Balancing
Frequency Handoff
AP Handoff
Band
2.4 GHz
802.11n/g/b
Channel Width
20MHz
Short Guard Interval
Channels
1
6
11
TX Power Control
Auto
Manual
TX Power
100%
SSIDs
Auto
Manual
example-staff (example-wifi)
Monitor Channel Utilization

Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

1. Go to *Network* > *Interfaces* and edit an unused interface.
   Set an *IP/Network Mask* and enable *CAPWAP* under *Administrative Access* > *IPv4*.
   Enable *DHCP Server*.
   Now connect the FortiAP unit to the this interface and apply power.
2. Go to *WiFi & Switch Controller* > *Managed FortiAPs*.
   Right-click on the FortiAP unit and select *Authorize*.
   Once authorized, right-click on the FortiAP unit again and select *Assign Profile* and select the FortiAP profile created earlier.



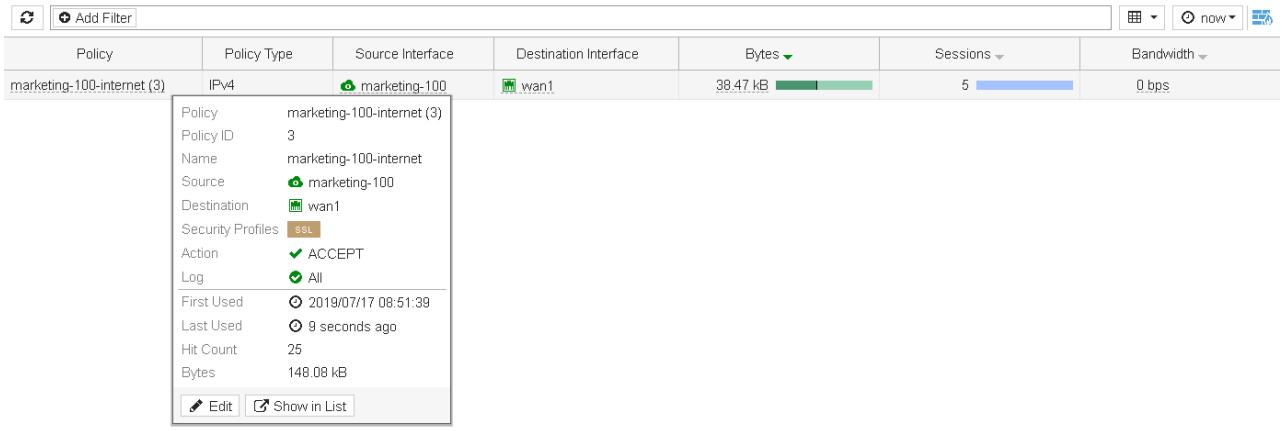
Results

The SSID will appear in the list of available wireless networks on the users' devices.

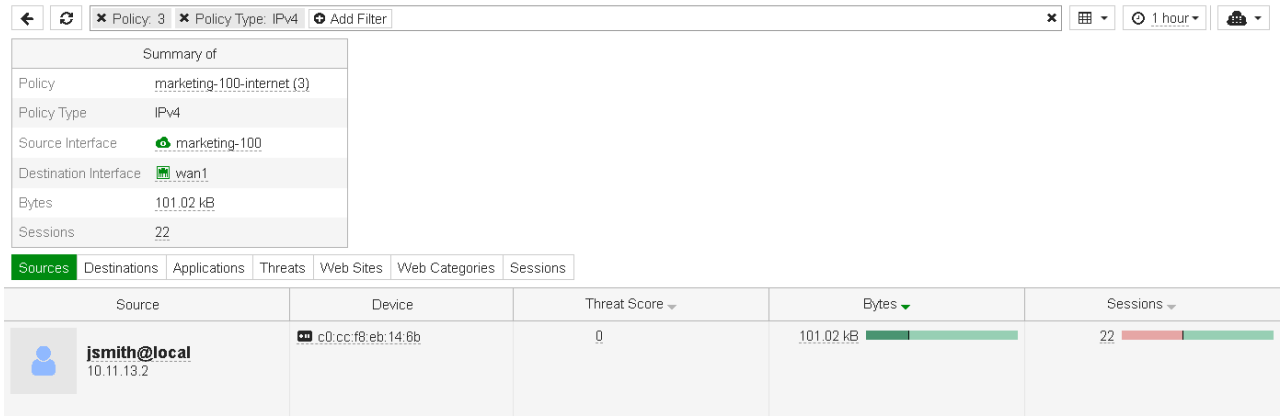
Both twhite and jsmith can connect to the SSID with their credentials and access the Internet.

If a certificate warning message appears, accept the certificate.

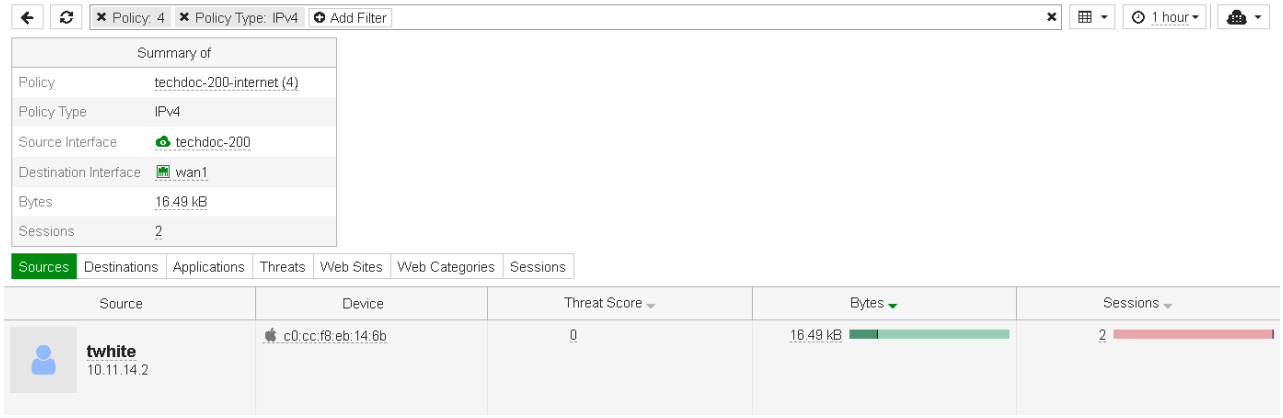
1. Go to *FortiView* > *Policies*.
   Note that traffic for jsmith and twhite will pass through different policies. In this example, the *marketing-100-internet* policy is displayed, indicating that jsmith has connected to the WiFi.



2. Double-click to drill-down, where the user's identity (including username, source IP, and device address) is confirmed.



3. When twhite has connected to the WiFi network, go to *FortiView* > *Policies* and drill-down. The user, and *techdoc-200-internet* policy, is confirmed.



WiFi using FortiAuthenticator RADIUS with certificates

This recipe will walk you through the configuration of FortiAuthenticator as the RADIUS server for a FortiGate wireless controller. WPA2-Enterprise with 802.1X authentication can be used to authenticate wireless users with FortiAuthenticator. 802.1X utilizes the Extensible Authentication Protocol (EAP) to establish a secure tunnel between participants involved in an authentication exchange.

EAP-TLS is the most secure form of wireless authentication because it replaces the client username/password with a client certificate. Every end user, including the authentication server, that participates in EAP-TLS must possess at least two certificates:

1. A client certificate signed by the certificate authority (CA)
2. A copy of the CA root certificate.

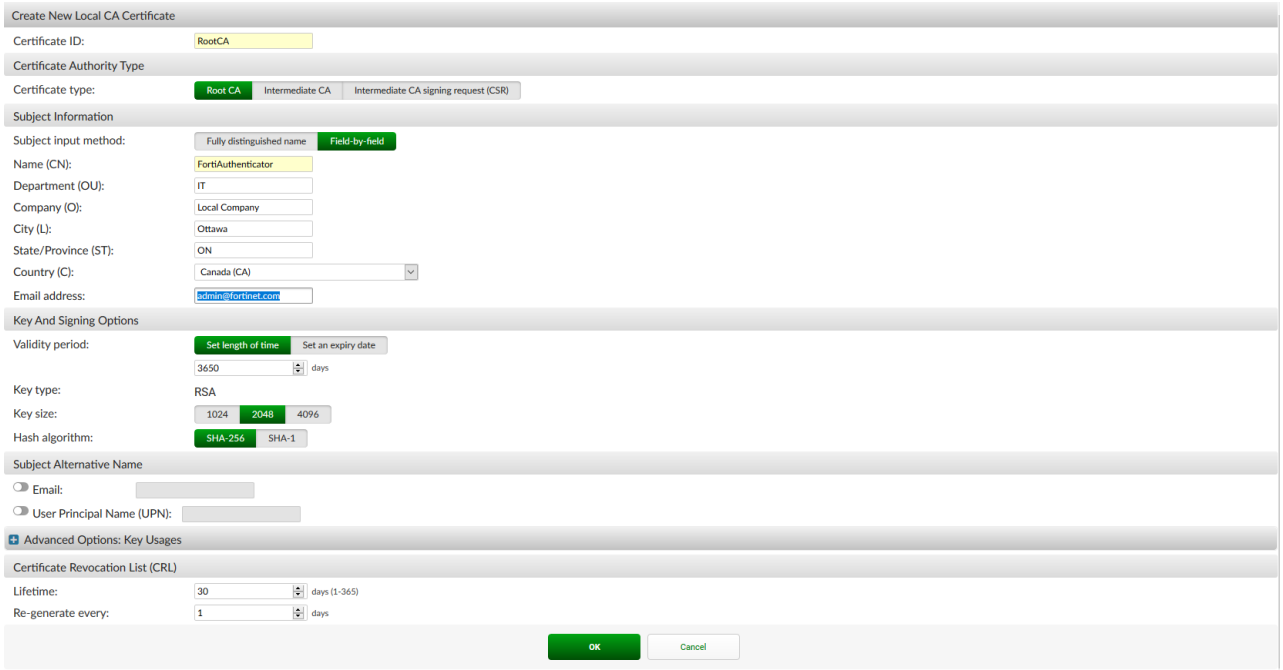
This recipe specifically focuses on the configuration of the FortiAuthenticator, FortiGate, and Windows 10 computer.

Creating a local CA on FortiAuthenticator

The FortiAuthenticator will act as the certificate authority for all certificates authenticated for client access. To enable this functionality, a self-signed root CA certificate must be generated.

To create the local CA:

1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Create New*.
   Configure the fields as required.

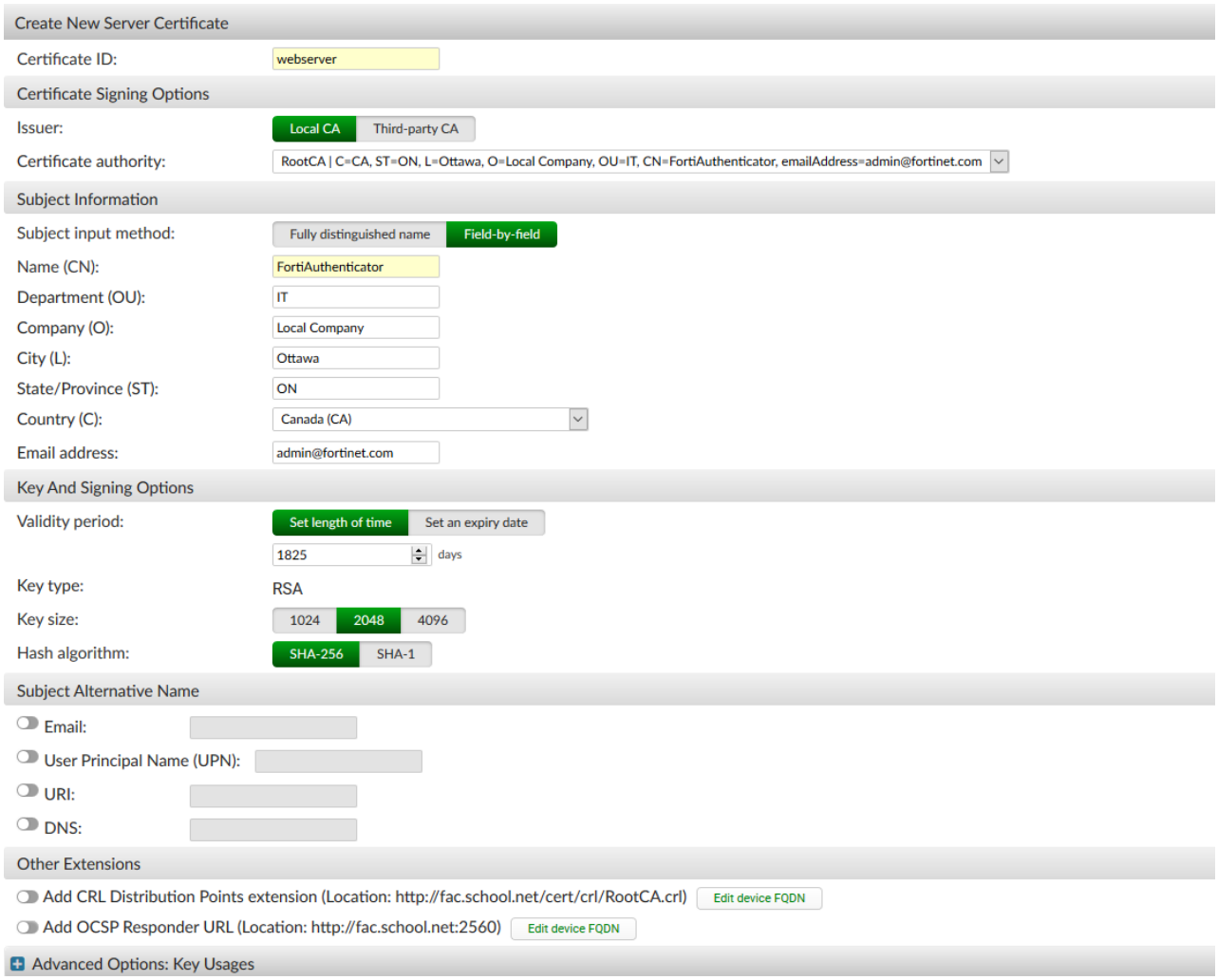


Creating a local service certificate on FortiAuthenticator

In order for the FortiAuthenticator to use a certificate in mutual authentication (supported by EAP-TLS), a local services certificate has to be created on behalf of the FortiAuthenticator.

To create the local service certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services* and select *Create New*. Complete the information in the fields pertaining to your organization.

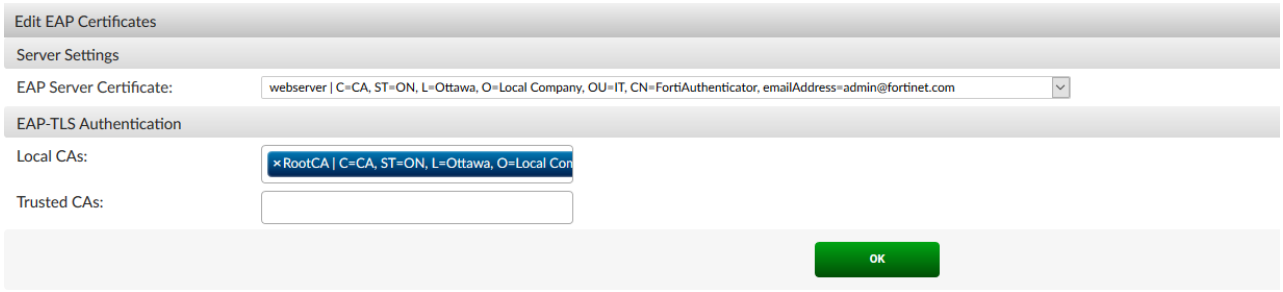


Configuring RADIUS EAP on FortiAuthenticator

In order for the FortiAuthenticator to present the newly created Local Services certificate as its authentication to the WiFi client, the RADIUS-EAP must be configured to use this certificate.

To configure RADIUS EAP on FortiAuthenticator:

1. Go to *Authentication* > *RADIUS Service* > *EAP,* and select *Create New*.
2. Select the corresponding Local Services certificate in the EAP Server Certificate section.
3. Choose the Local CA certificate previous configured in the Local CAs section.

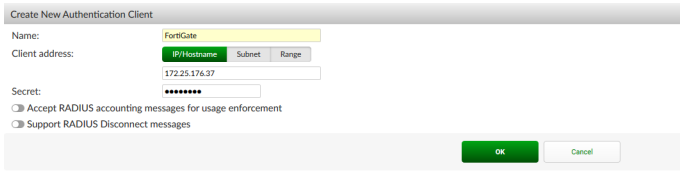


Configuring RADIUS client on FortiAuthenticator

The FortiAuthenticator has to be configured to allow RADIUS clients to make authorization requests to it.

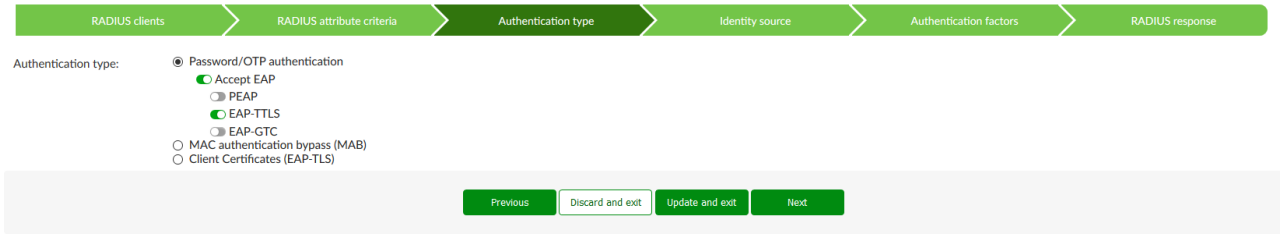
To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.



To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable *Accept EAP* with only *EAP-TTLS* selected.
   EAP-TLS should be the only EAP type selected to prevent fallback to a less secure version of authentication if a certificate is not presented by the WiFi client.



5. Choose a username format (in this example: *username@realm*), select the *Local* realm.

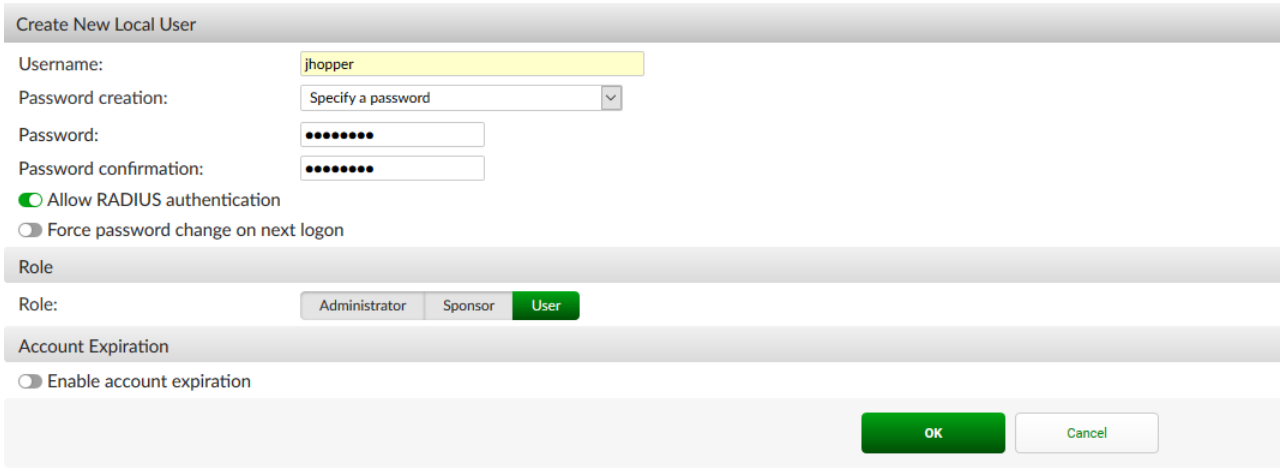
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

Configuring local user on FortiAuthenticator

The authentication of the WiFi client will be tied to a user account on the FortiAuthenticator. In this scenario, a local user will be configured but remote users associated with LDAP can be configured as well.

To configure a local user:

1. Go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
   Fill out applicable user information.

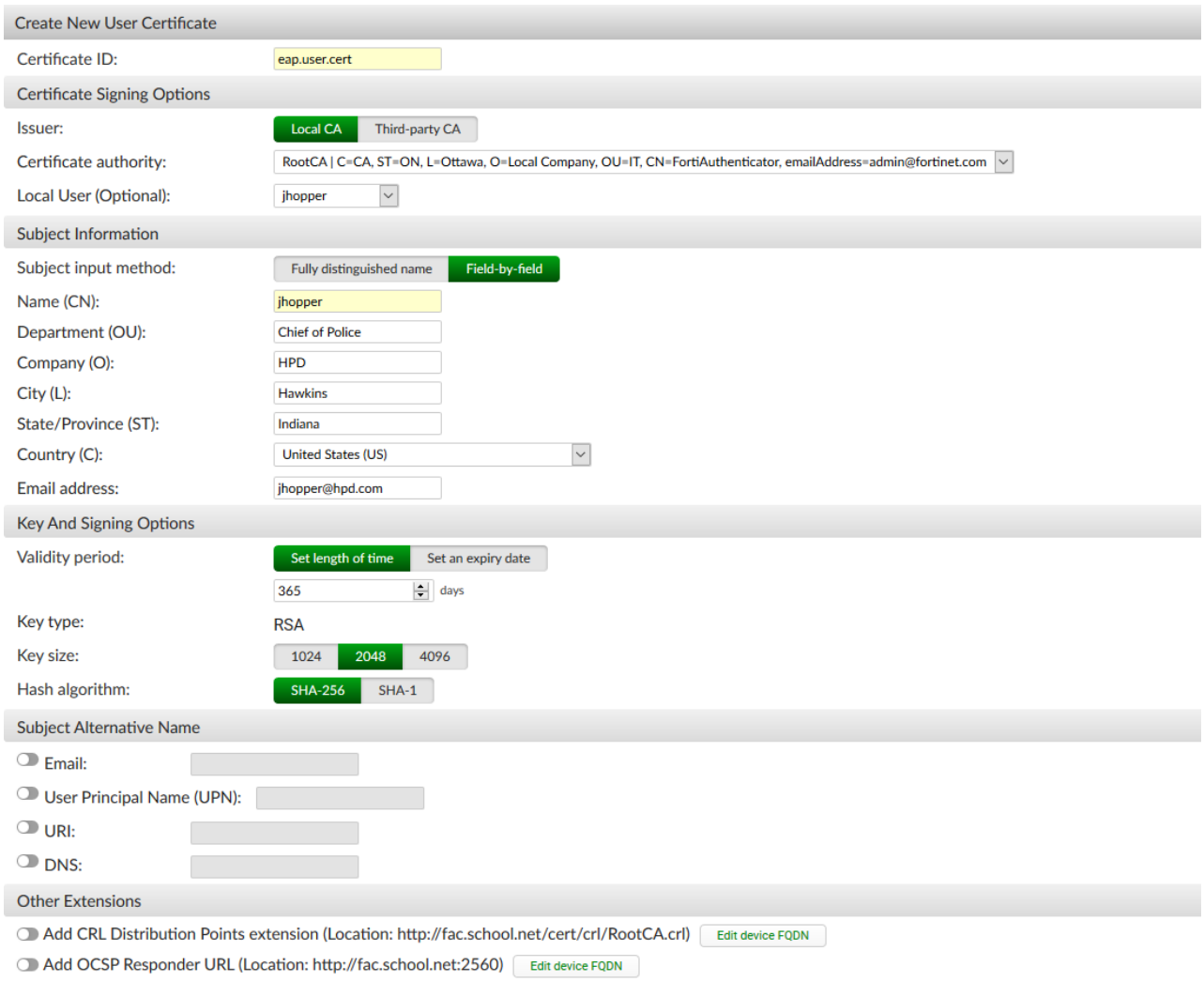


Configuring local user certificate on FortiAuthenticator

The certificate created locally on the FortiAuthenticator will be associated with the local user. It is important to note that the *Name (CN)* must match the username exactly of the user that is registered in the FortiAuthenticator (in the example, *eap-user*).

To configure the local user certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Create New*.
   Fill out applicable user information to map the certificate to the correct user.



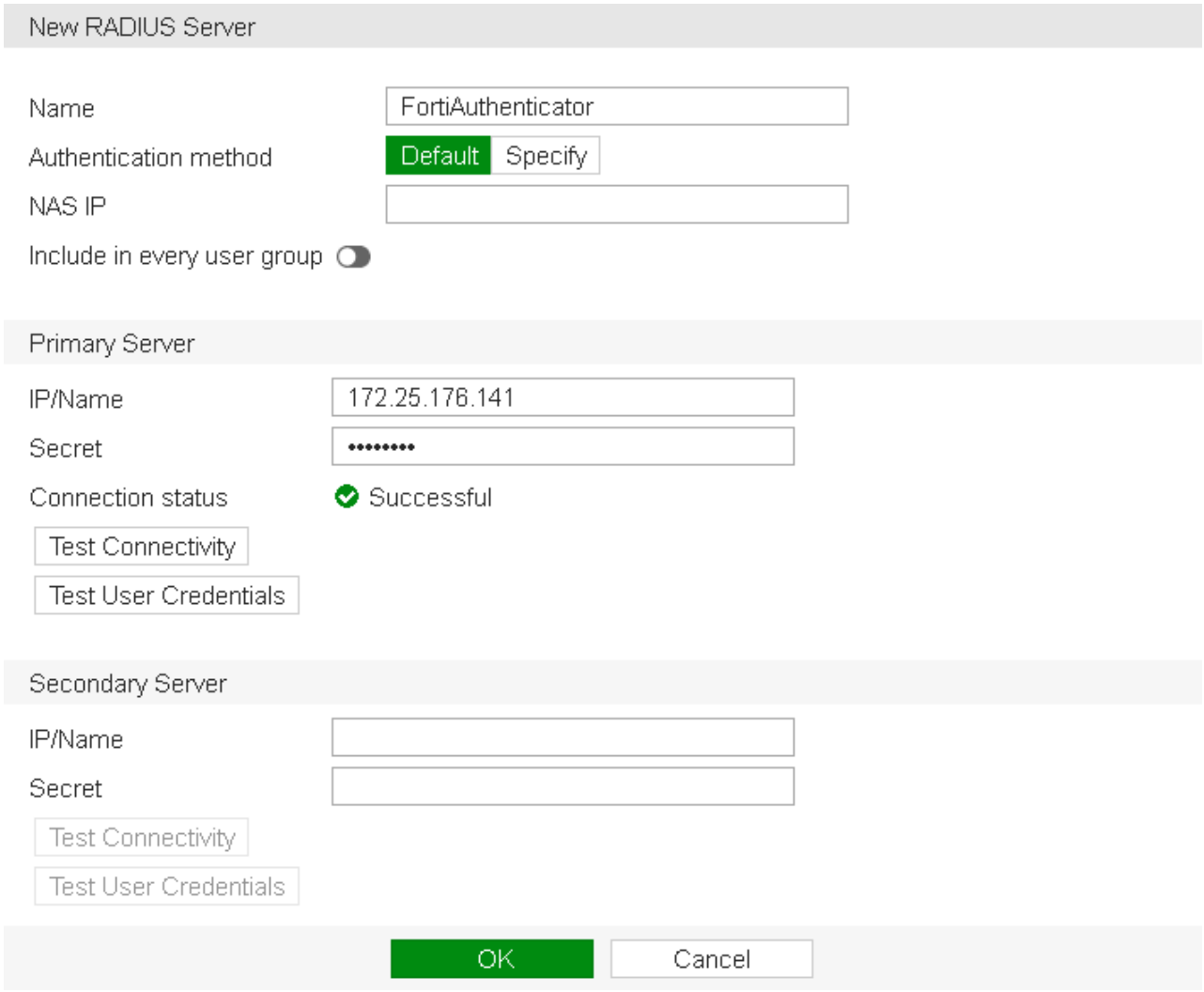
Creating RADIUS server on FortiGate

In order to proxy the authentication request from the wireless client, the FortiGate will need to have a RADIUS server to submit the authentication request to.

To create the RADIUS server on FortiGate:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*. Enter a *Name*, the FortiAuthenticator's IP address, and the same *Secret* set on the FortiAuthenticator.

Select *Test Connectivity* to confirm the successful connection.

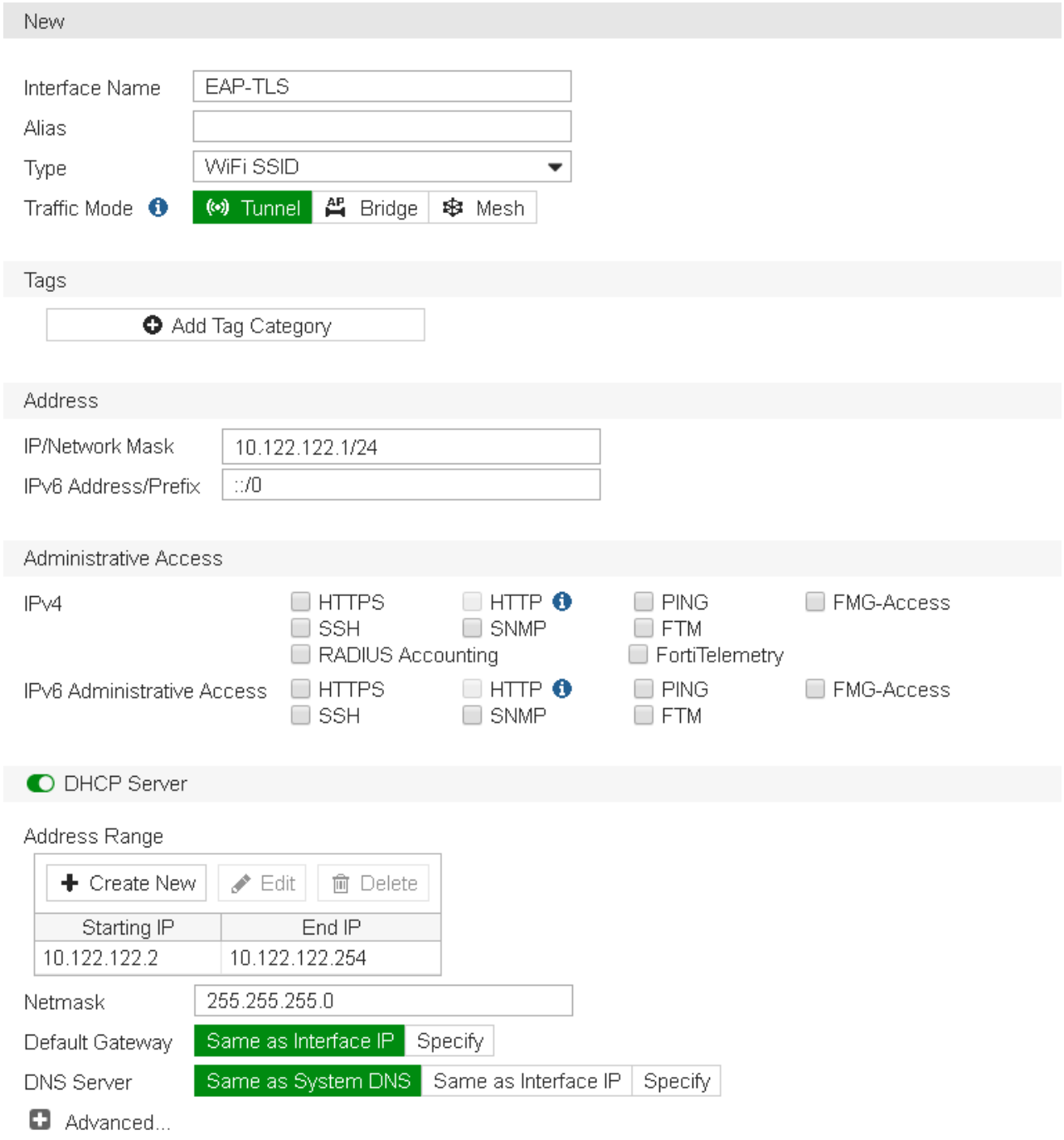


Creating WiFi SSID on FortiGate

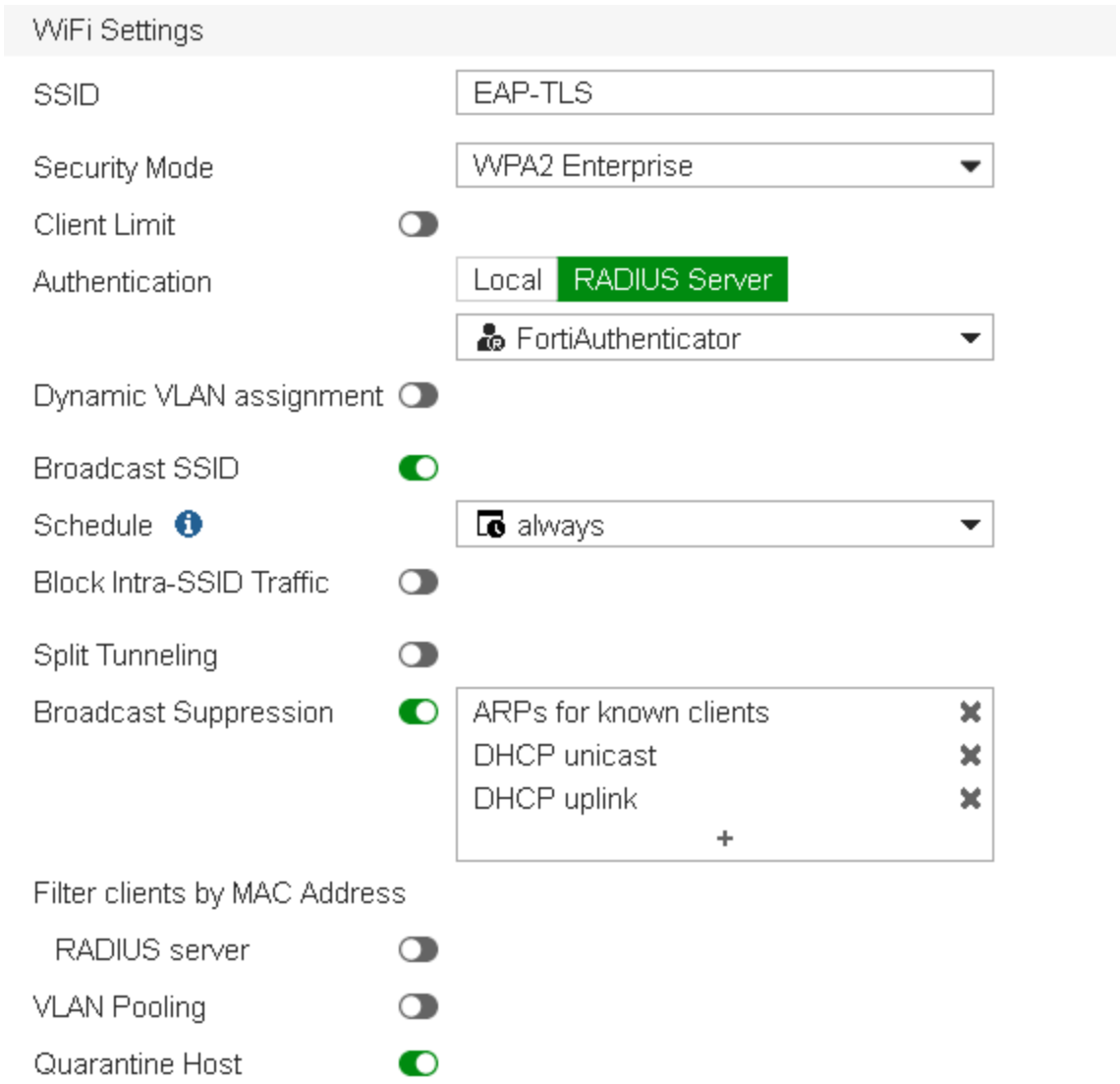
In order for the WiFi client to connect using its certificate a SSID has to be configured on the FortiGate to accept this type of authentication.

To create the WiFi SSID:

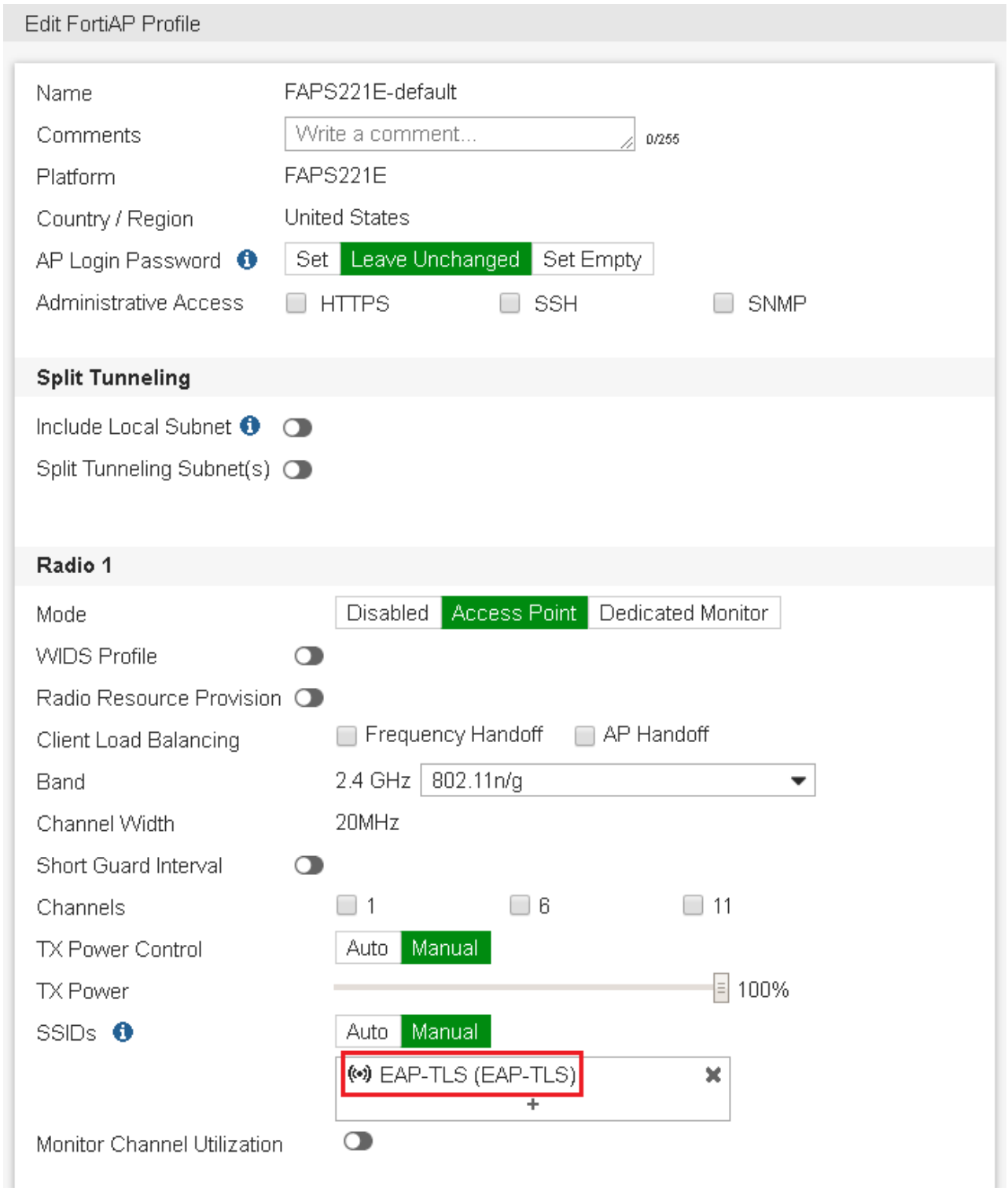
1. Go to *WiFi & Switch Controller* > *SSID* and create an SSID with DHCP for clients.



2. Set the following *WiFi Settings*, assigning the *RADIUS Server* configured earlier.



3. Then go to *WiFi & Switch Controller* > *FortiAP Profiles* and edit your FortiAP default profile. Select the new SSID for both *Radio 1* and *Radio 2*.



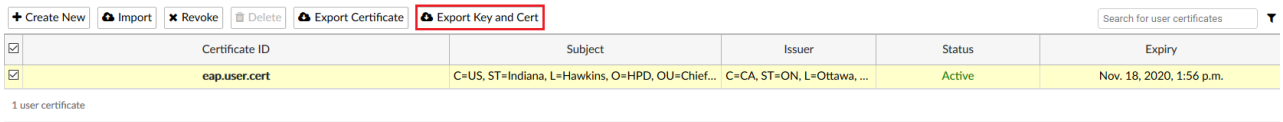
4. Then go to *Policy & Objects* > *IPv4 Policy* and create a policy that allows outbound traffic from the *EAP-TLS* wireless interface to the Internet.

Exporting user certificate from FortiAuthenticator

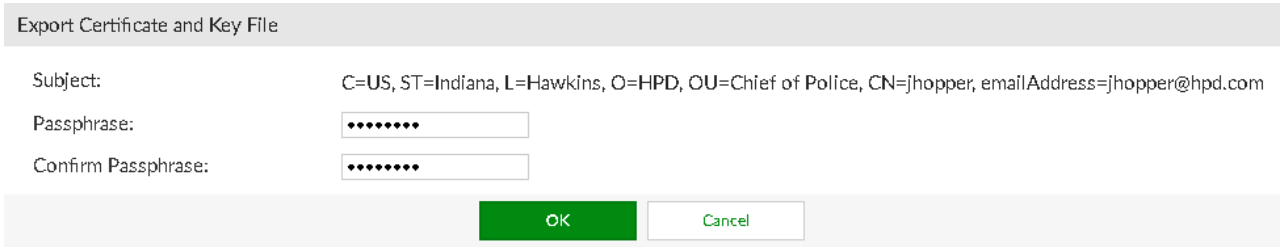
In order for the WiFi client to authenticate with the RADIUS server, the user certificate created in the FortiAuthenticator must first be exported.

To export the FortiAuthenticator user certificate:

1. On the FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users*. Select the certificate and select *Export Key and Cert*.



2. In the *Export User Certificate and Key File* dialog, enter and confirm a *Passphrase*. This password will be used when importing the certificate into a Windows 10 computer. Select *OK*.

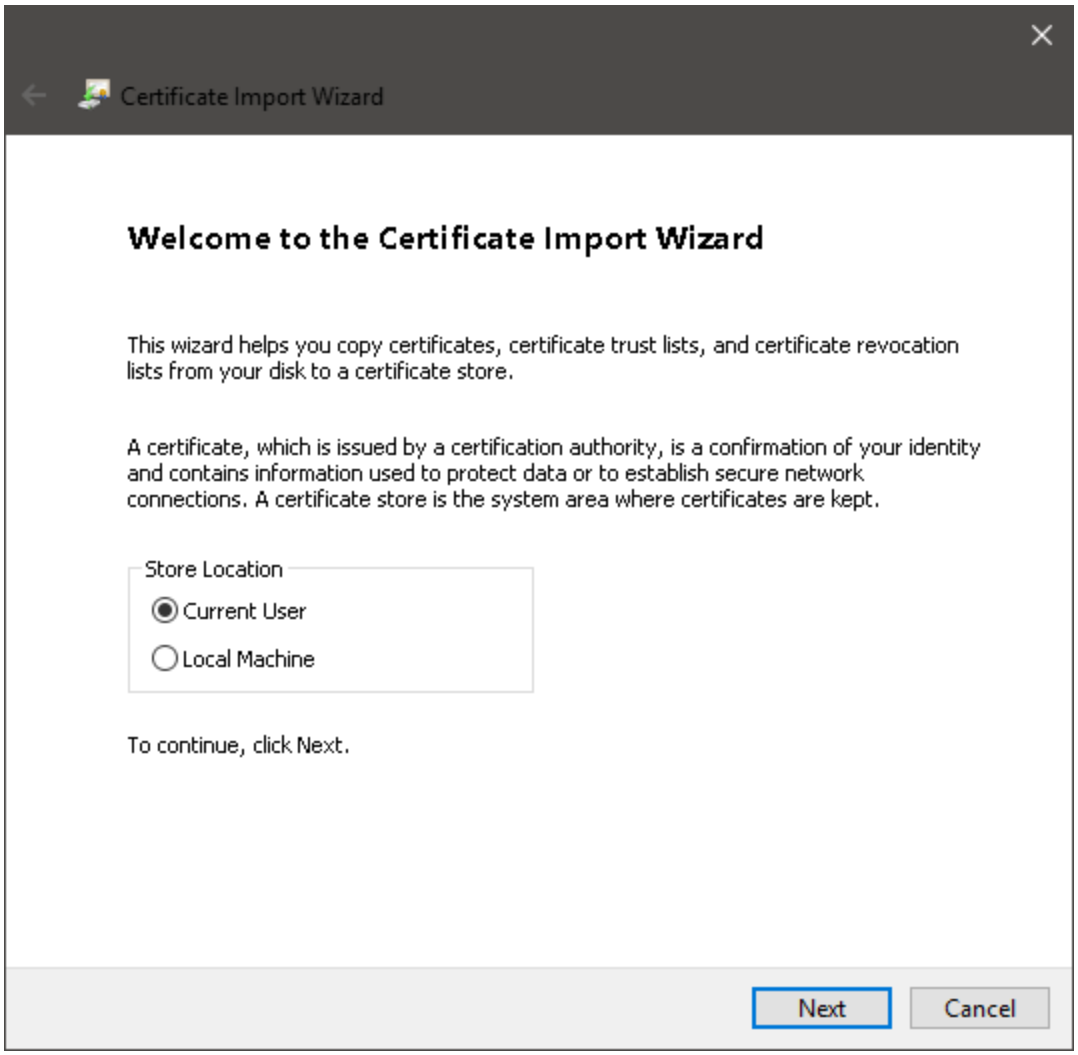


3. Select *Download PKCS#12 file* to pull this certificate to the Widows 10 computer. Select *Finish*.

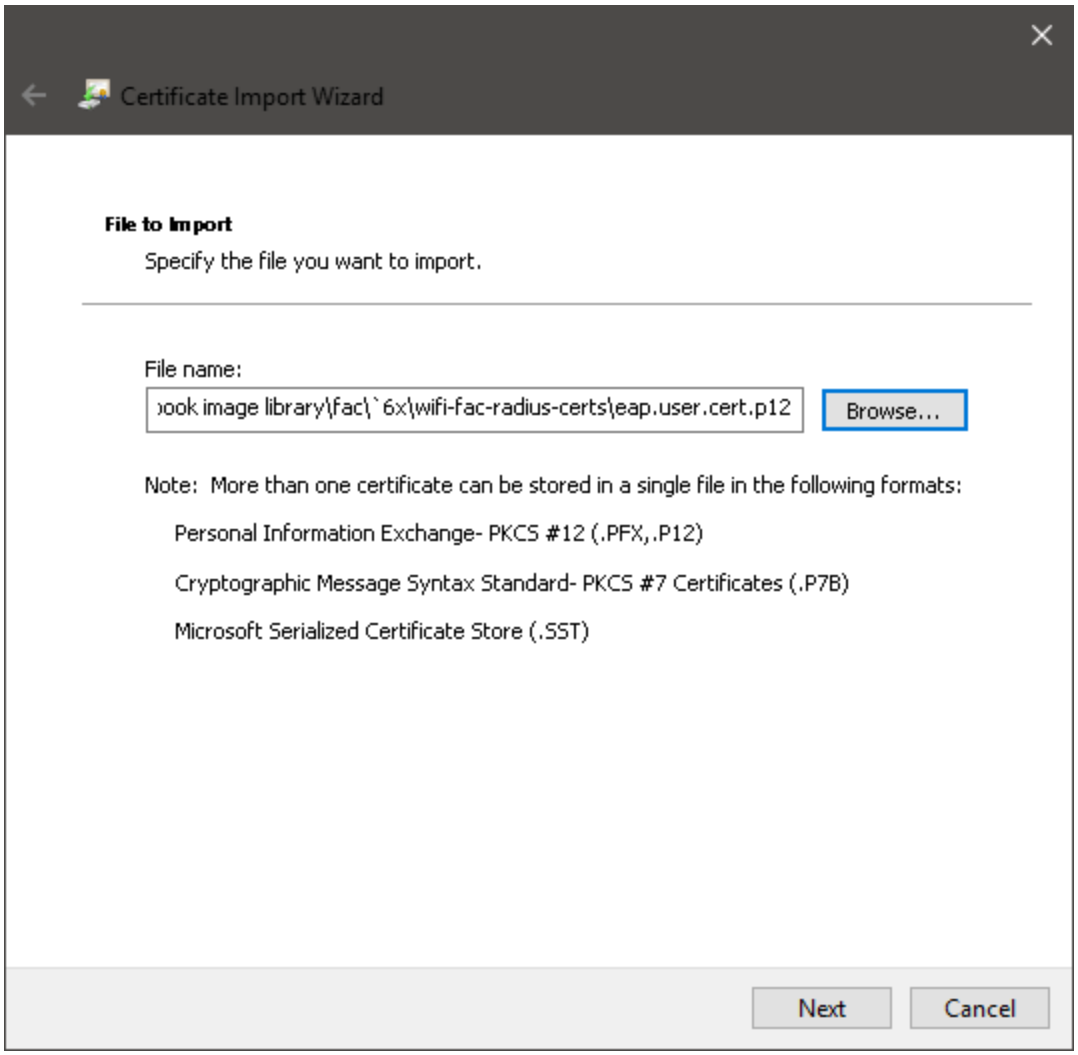
Importing user certificate into Windows 10

To import the user certificate:

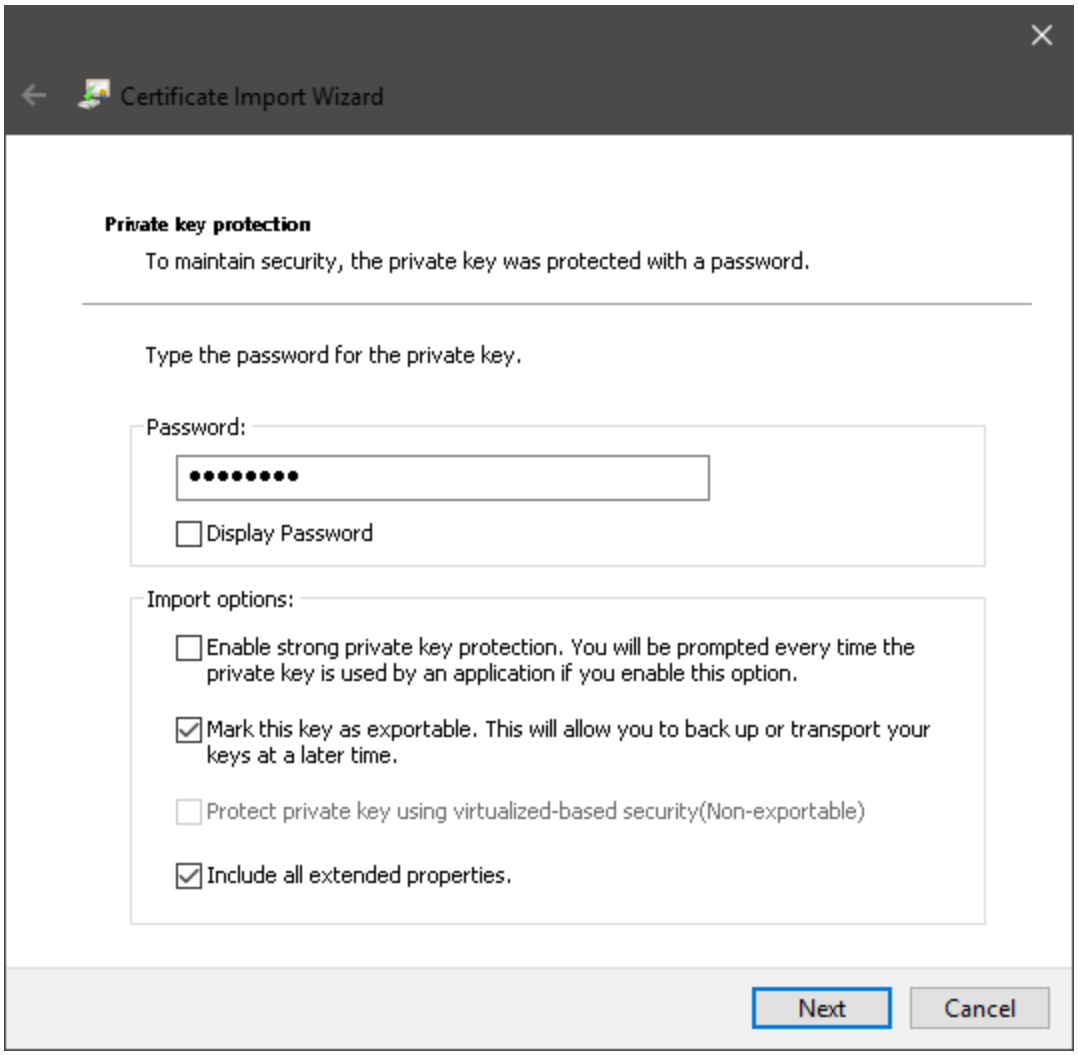
1. On the Windows 10 computer, double-click the downloaded certificate file from the FortiAuthenticator. This will launch the *Certificate Import Wizard*. Select *Next*.



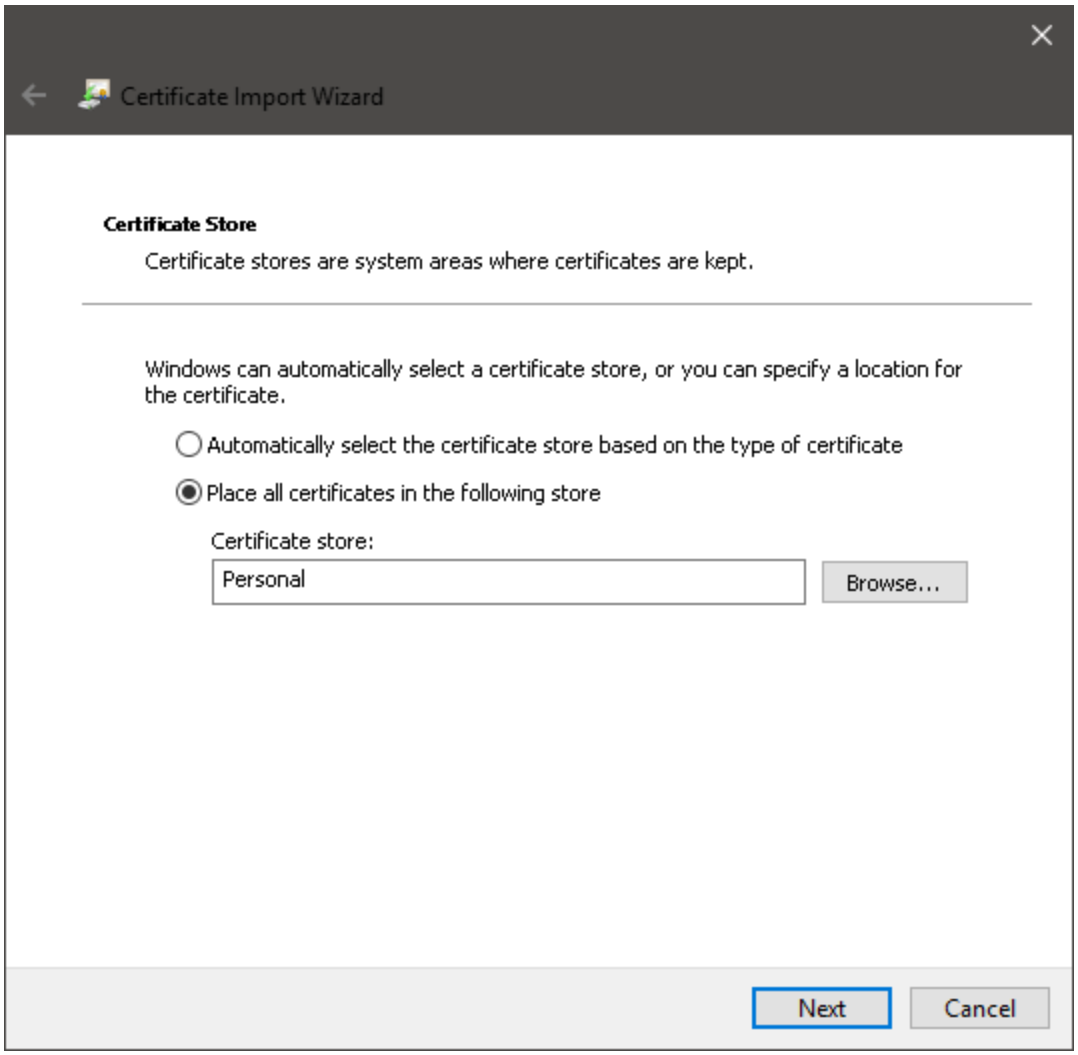
2. Make sure the correct certificate is shown in the *File name* section in the *File to Import* window. Select *Next*.



3. Enter the *Password* created on the FortiAuthenticator during the export of the certificate. Select *Mark this key as exportable* and leave the remaining options to default. Select *Next*.



4. In the *Certificate Store*, choose the *Place all certificates in the following store*.
   Select *Browse* and choose *Personal*. Select *Next*, and then *Finish*.
   A dialog box will show up confirming the certificate was imported successfully.

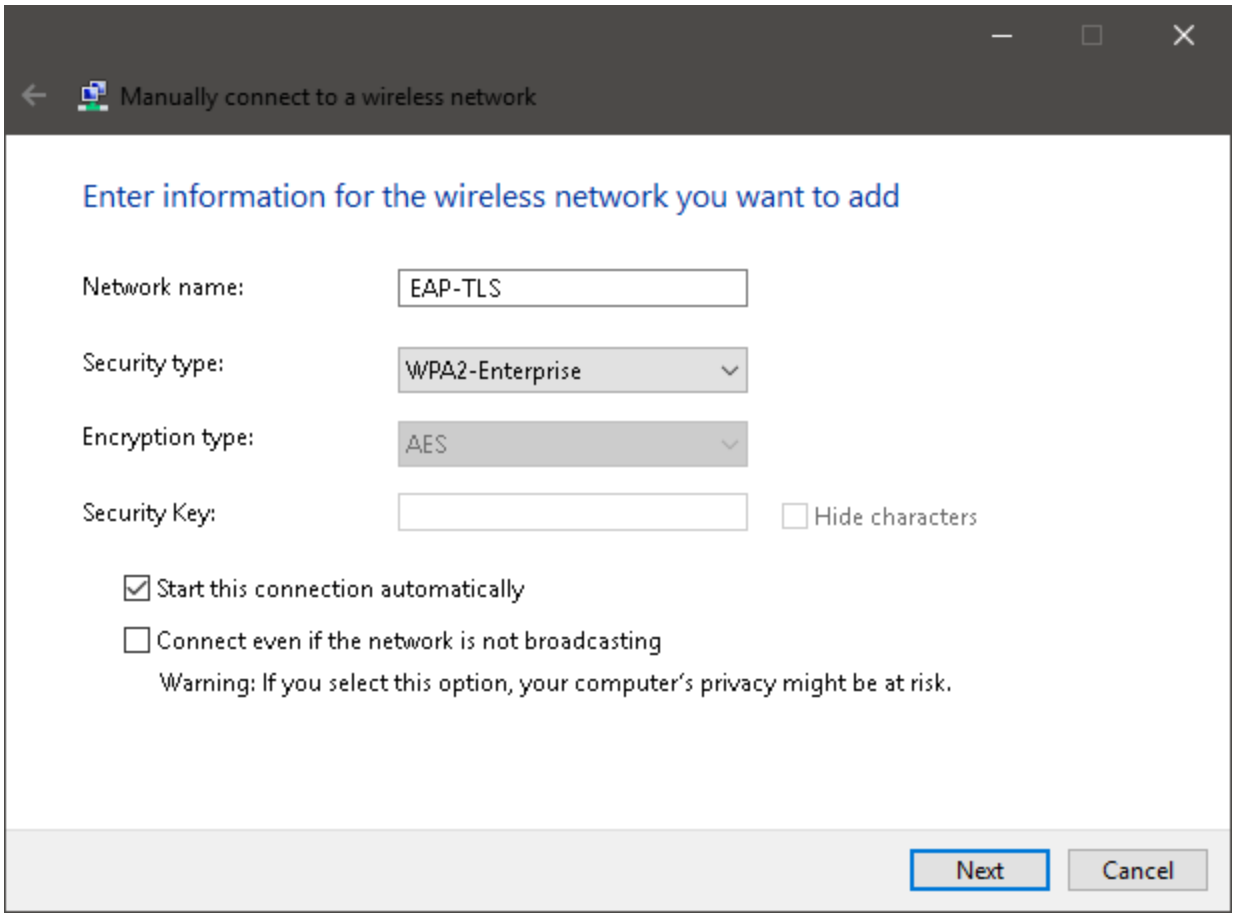


Configuring Windows 10 wireless profile to use certificate

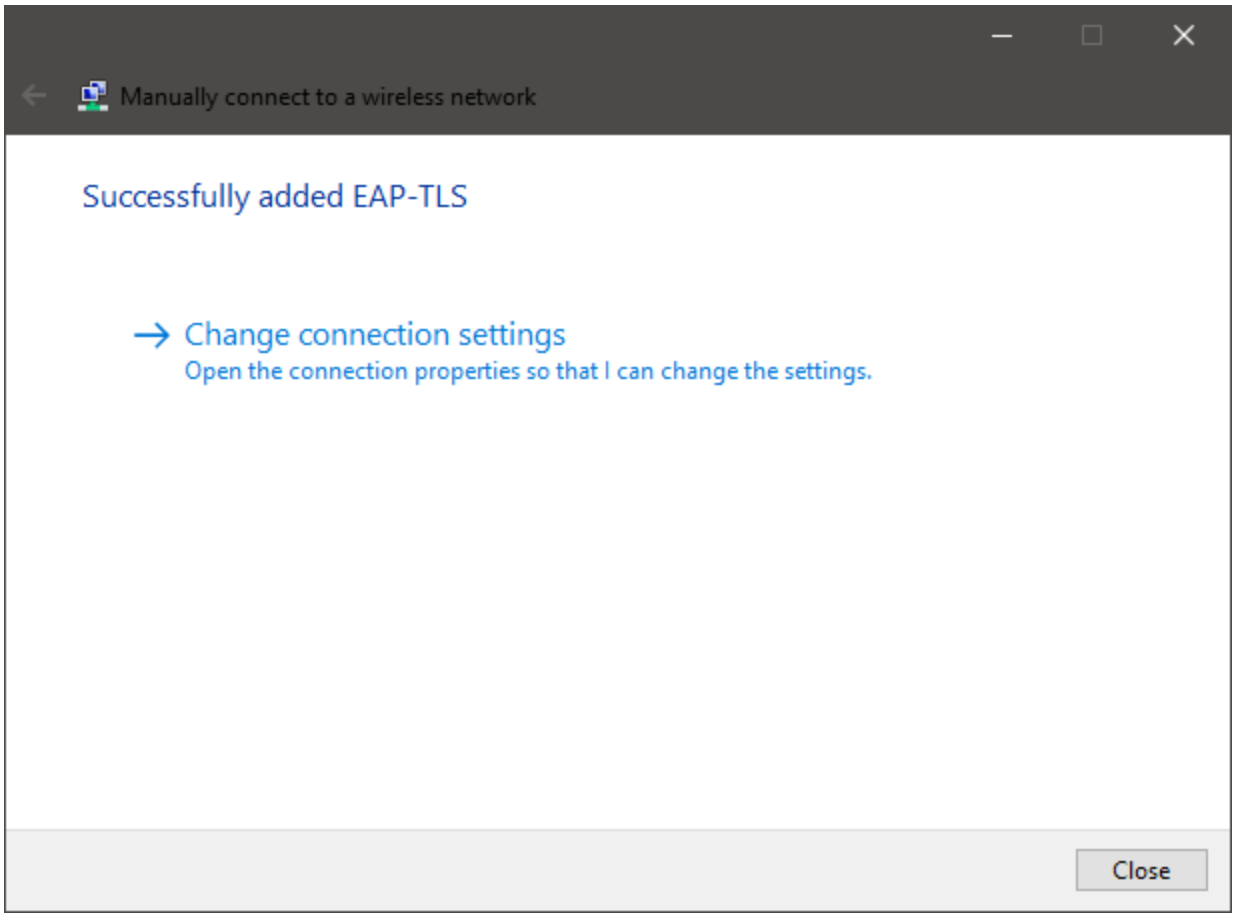
Create a new wireless SSID for this secure connection, in this case EAP-TLS.

To create a wireless SSID:

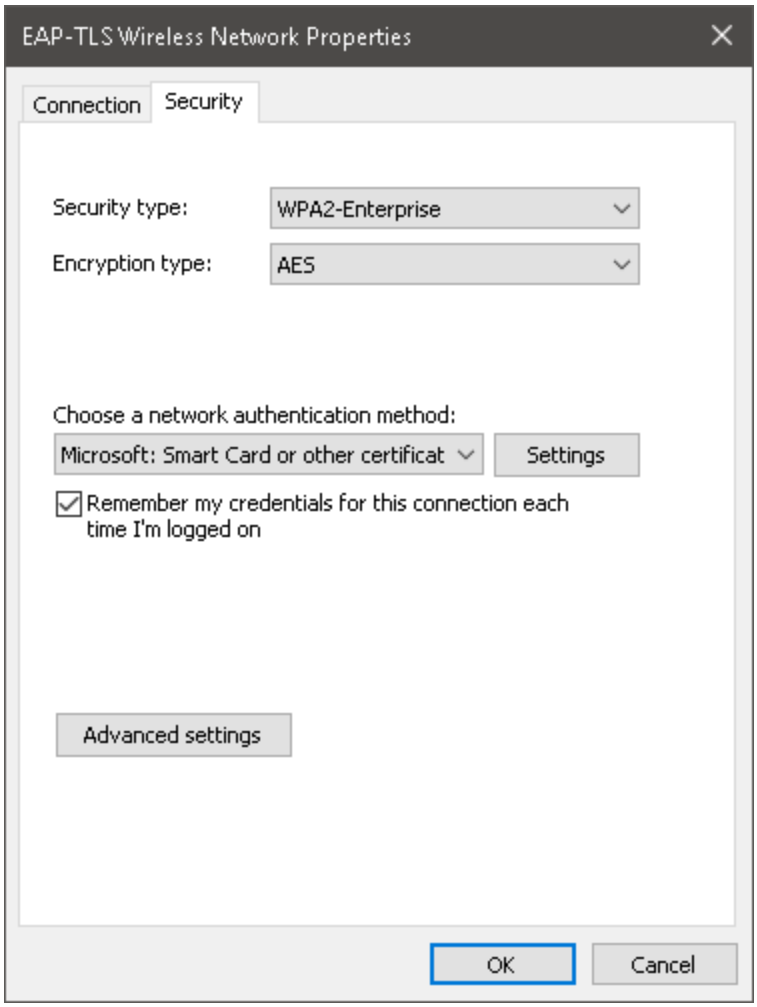
1. On Windows 10, got to *Control Panel* > *Network and Sharing Center* > *Set up a new connection or network* > *Manually connect to a wireless network*. Enter a *Network name* and set *Security type* to *WPA2-Enterprise*. The *Encryption type* is set to *AES*.



2. Once created, you have the option to modify the wireless connection. Select *Change connection settings*.

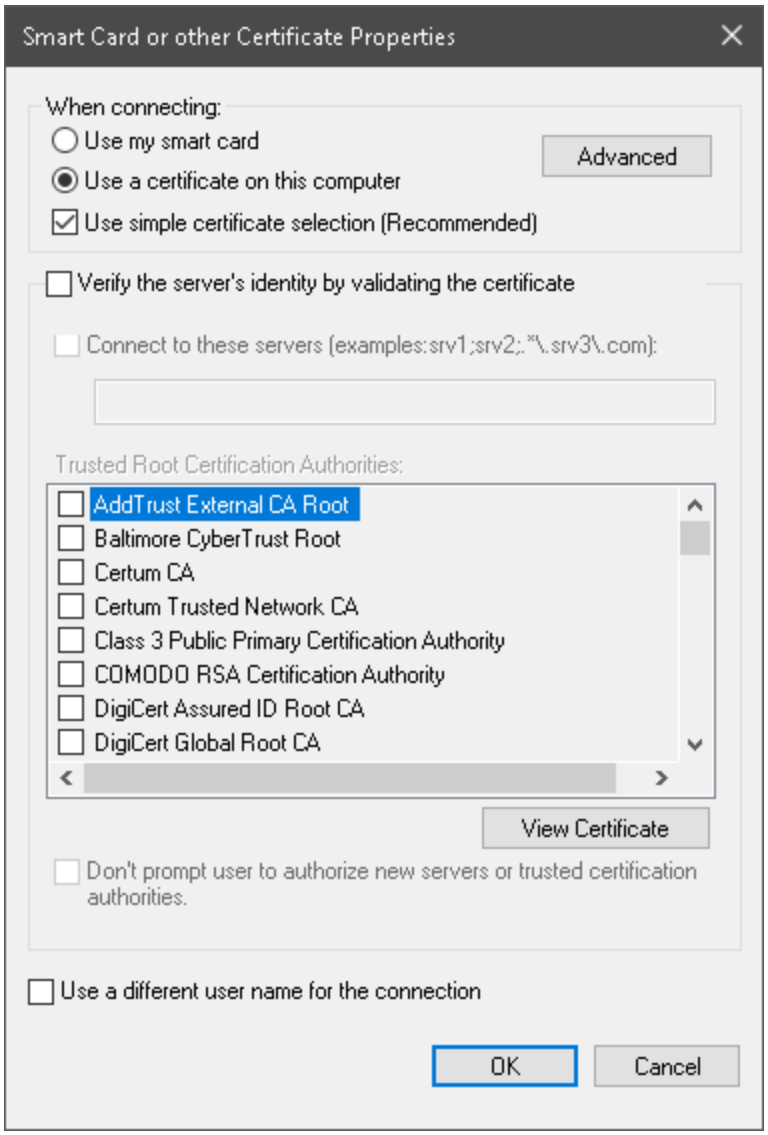


3. In the *Security* tab, set *Choose a network authentication method* to *Microsoft: Smart card or other certificates*, and select *Settings*.



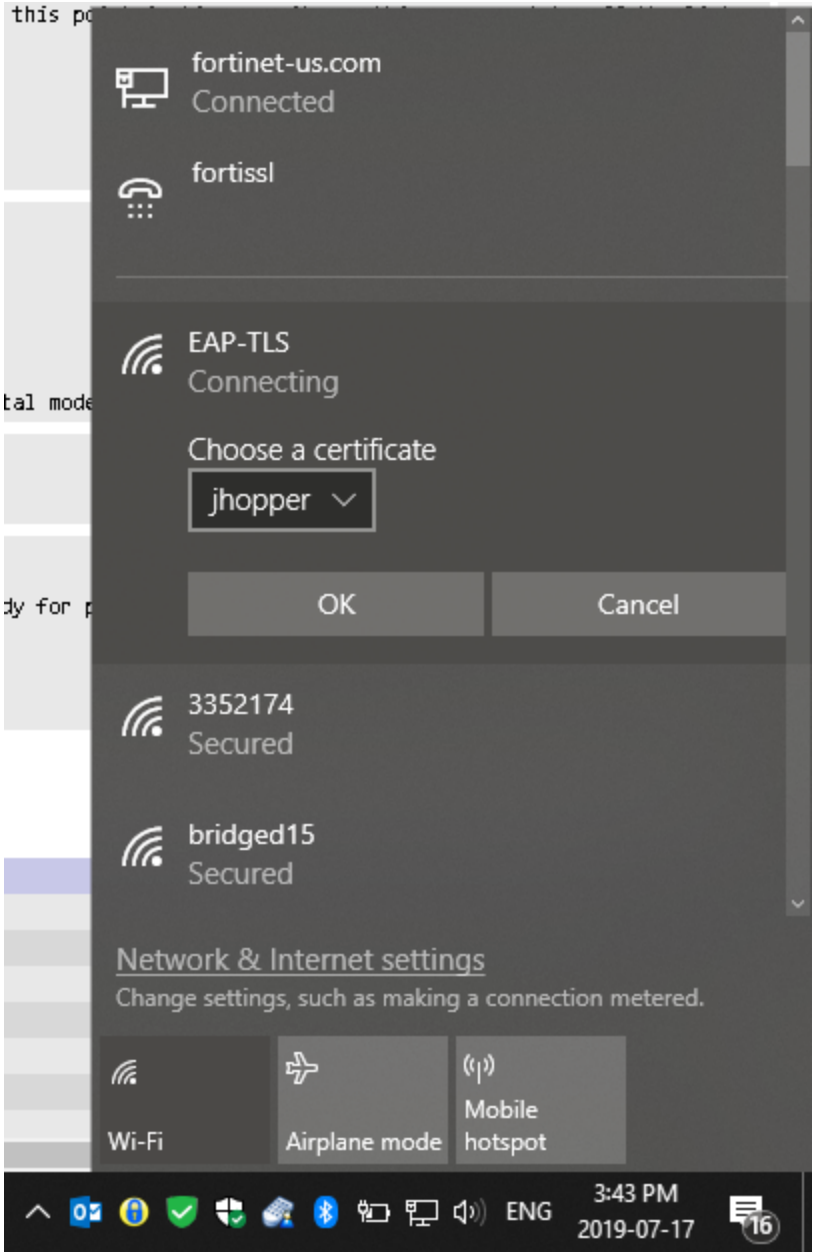
4. Enable both *Use a certificate on this computer* and *Use simple certificate selection*.
   Note that, for simplification purposes, *Verify the server's identity by validating the certificate* has been disabled. However EAP--TLS allows the client to validate the server as well as the server validate the client. To enable this, you will need to import the CA from the FortiAuthenticator to the Windows 10 computer and make sure that it is enabled as a Trusted Root Certification Authority.

   Select *OK* for all dialog windows to confirm all settings. The configuration for the Windows 10 computer has been completed and the user should be able to authenticate to WiFi via the certificate without using their username and password.

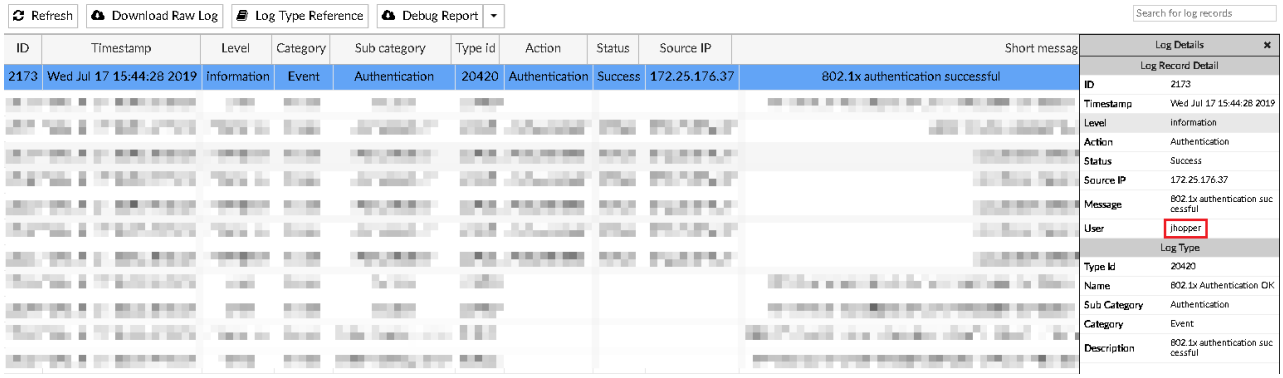

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Advanced
Use simple certificate selection (Recommended)
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AddTrust External CA Root
Baltimore CyberTrust Root
Certum CA
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
View Certificate
Don't prompt user to authorize new servers or trusted certification authorities.
Use a different user name for the connection
OK
Cancel

Results

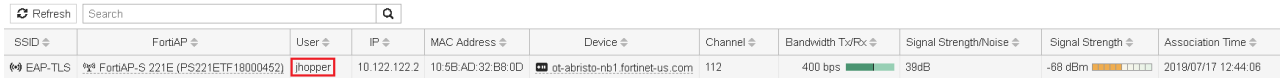
1. On the user's device, attempt to connect to the WiFi. Select the user's certificate and select *OK*.



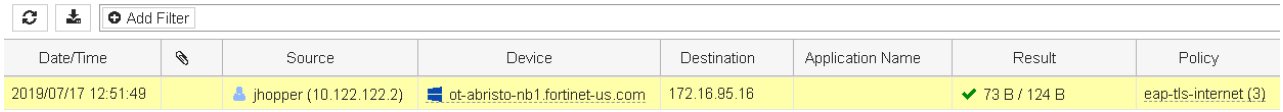
2. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the successful authentication.

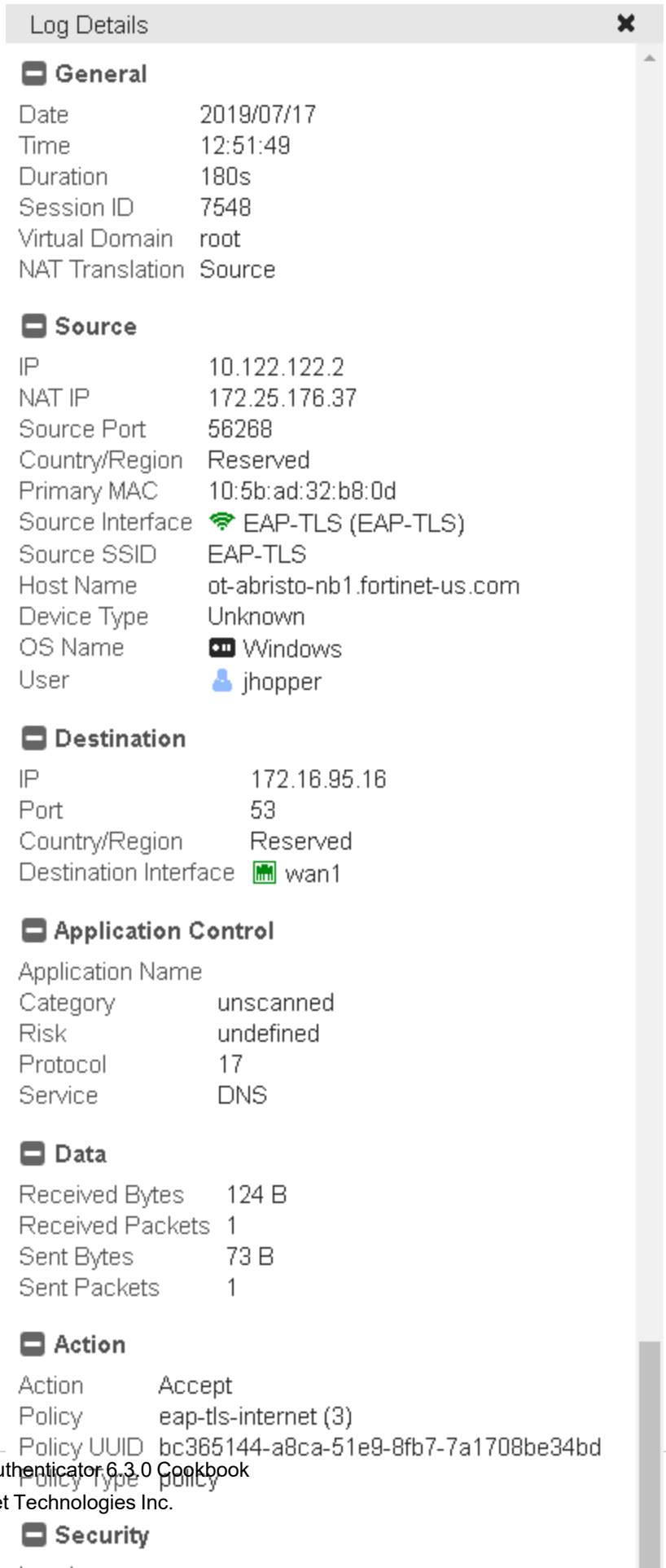


3. On the FortiGate, go to **Monitor > WiFi Client Monitor** to view various information about the client.

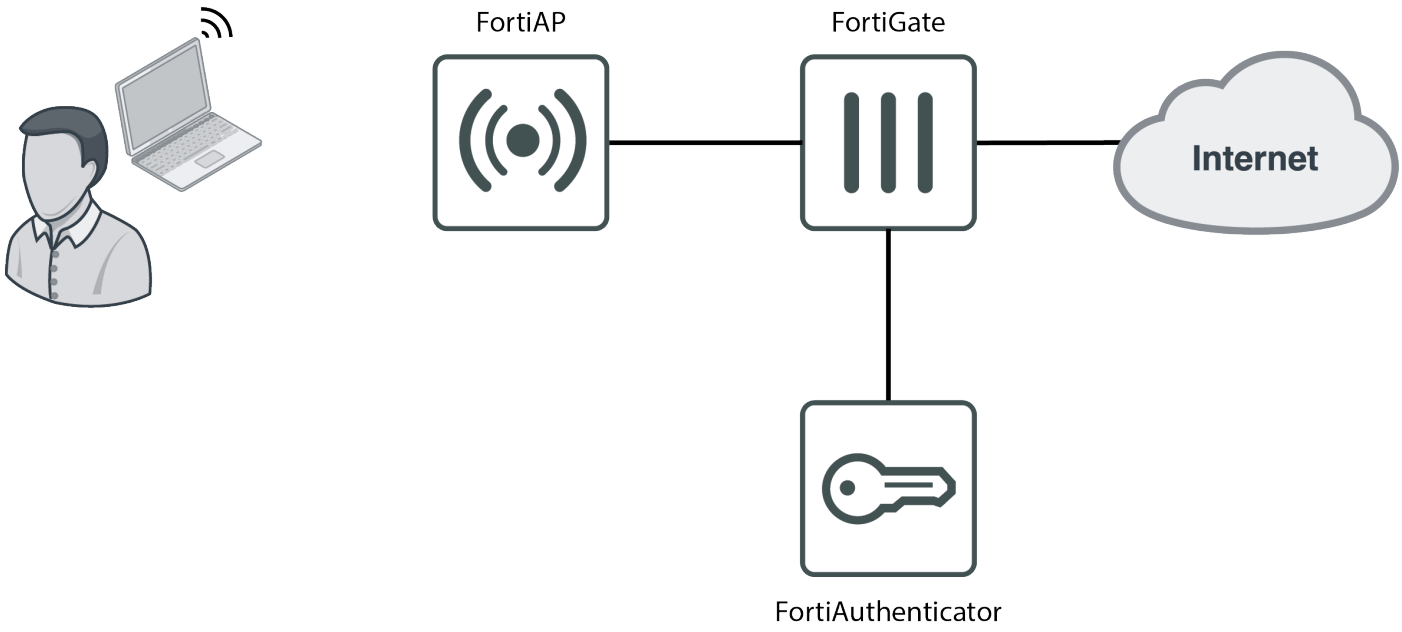


You can also go to *Log & Report > Forward Traffic* to view more log details.




Log Details
General
Date 2019/07/17
Time 12:51:49
Duration 180s
Session ID 7548
Virtual Domain root
NAT Translation Source
Source
IP 10.122.122.2
NAT IP 172.25.176.37
Source Port 56268
Country/Region Reserved
Primary MAC 10:5b:ad:32:b8:0d
Source Interface EAP-TLS (EAP-TLS)
Source SSID EAP-TLS
Host Name ot-abristo-nb1.fortinet-us.com
Device Type Unknown
OS Name Windows
User jhopper
Destination
IP 172.16.95.16
Port 53
Country/Region Reserved
Destination Interface wan1
Application Control
Application Name
Category unscanned
Risk undefined
Protocol 17
Service DNS
Data
Received Bytes 124 B
Received Packets 1
Sent Bytes 73 B
Sent Packets 1
Action
Action Accept
Policy eap-tls-internet (3)
Policy UUID bc365144-a8ca-51e9-8fb7-7a1708be34bd
Policy Type policy
Security

WiFi RADIUS authentication with FortiAuthenticator



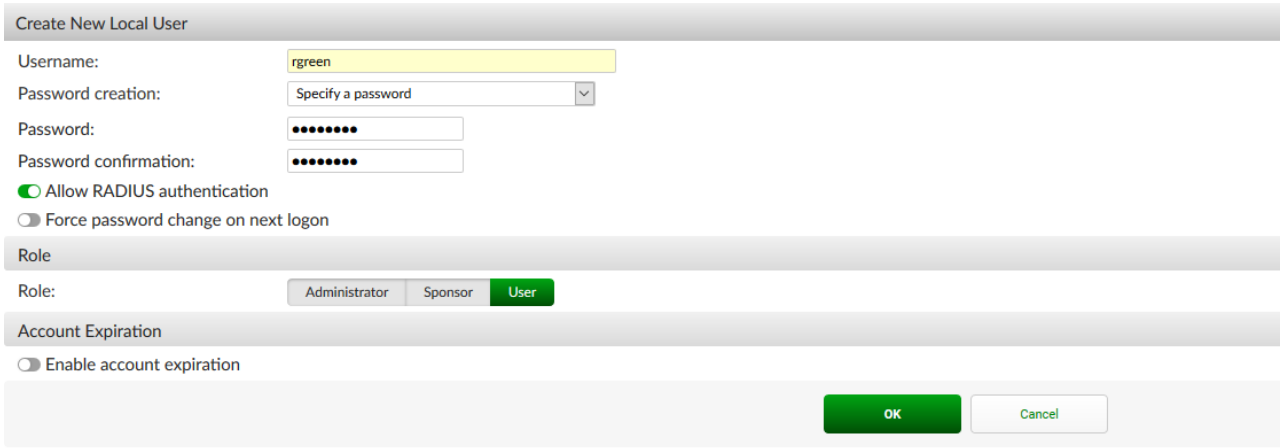
In this example, you use a RADIUS server to authenticate your WiFi clients.

The RADIUS server is a FortiAuthenticator that is used authenticate users who belong to the employees user group.

Creating users and user groups on the FortiAuthenticator

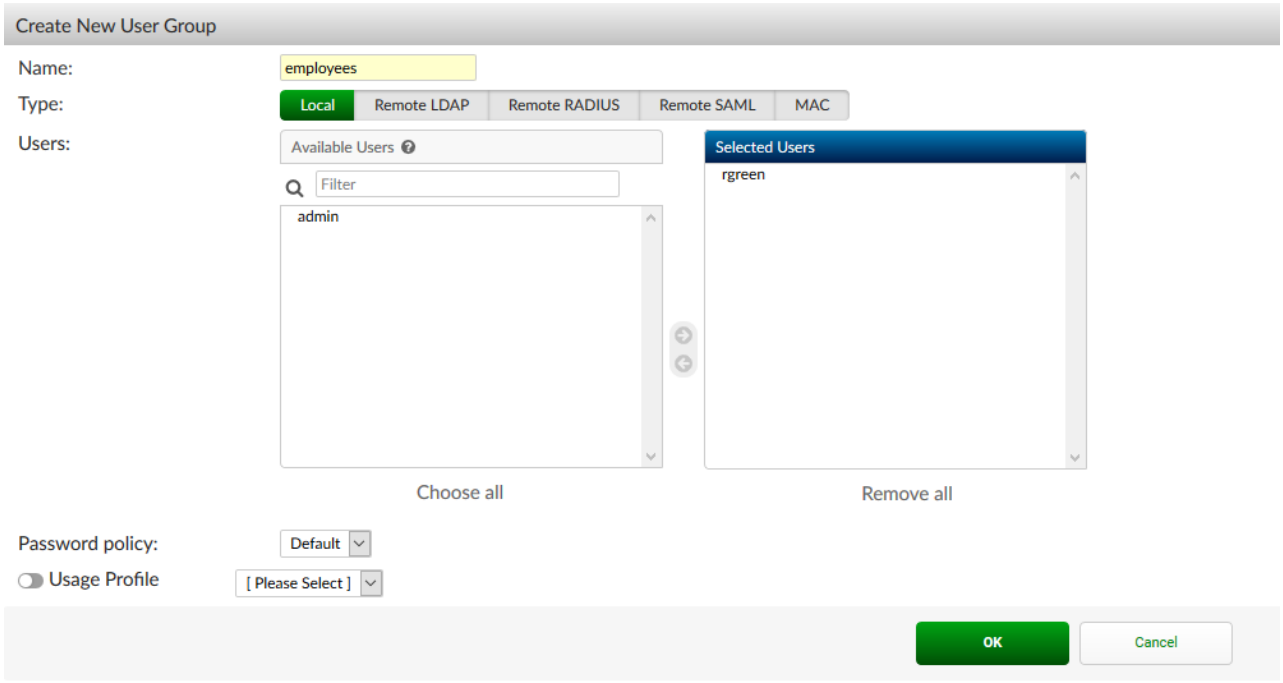
To create users and user groups:

1. Go to *Authentication* > *User Management* > *Local Users* and create a user account.



2. Then go to *Authentication* > *User Management* > *User Groups* and create a local user group (employees), adding

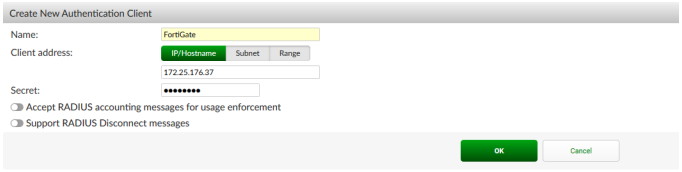
the newly created user.



Registering the FortiGate as a RADIUS client on the FortiAuthenticator

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.



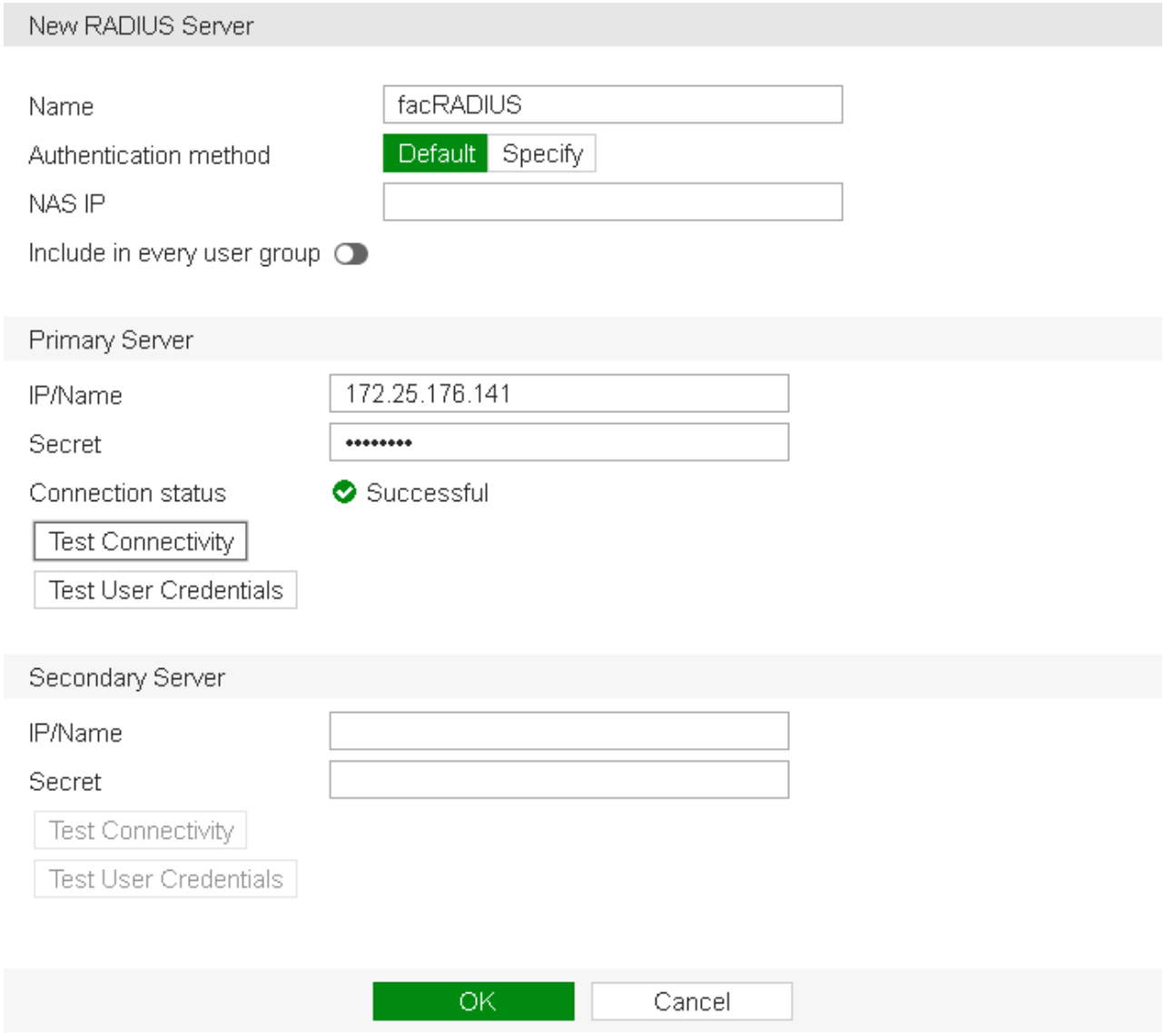
To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable all *EAP* types.
5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
   Add the user group *employees* as a filter.
6. Review the remaining configurations, and click *Save and Exit*.

Configuring FortiGate to use the RADIUS server

To configure FortiGate to use the RADIUS server:

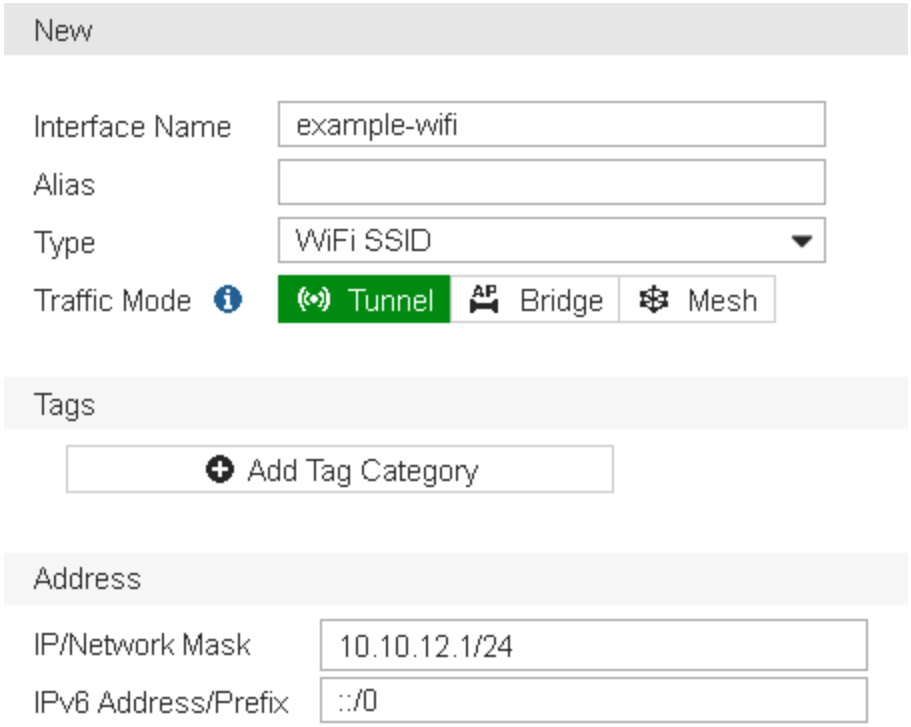
1. Go to *User & Device* > *RADIUS Servers* and add the FortiAuthenticator as a RADIUS server. Select *Test Connectivity* to confirm the successful connection.



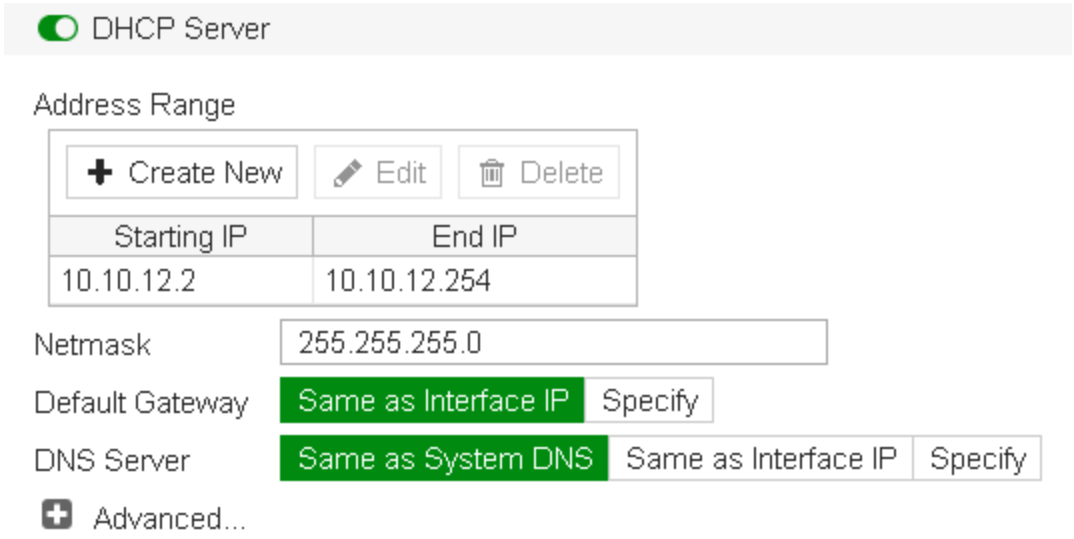
Creating SSID and set up authentication

To create an SSID and set up authentication:

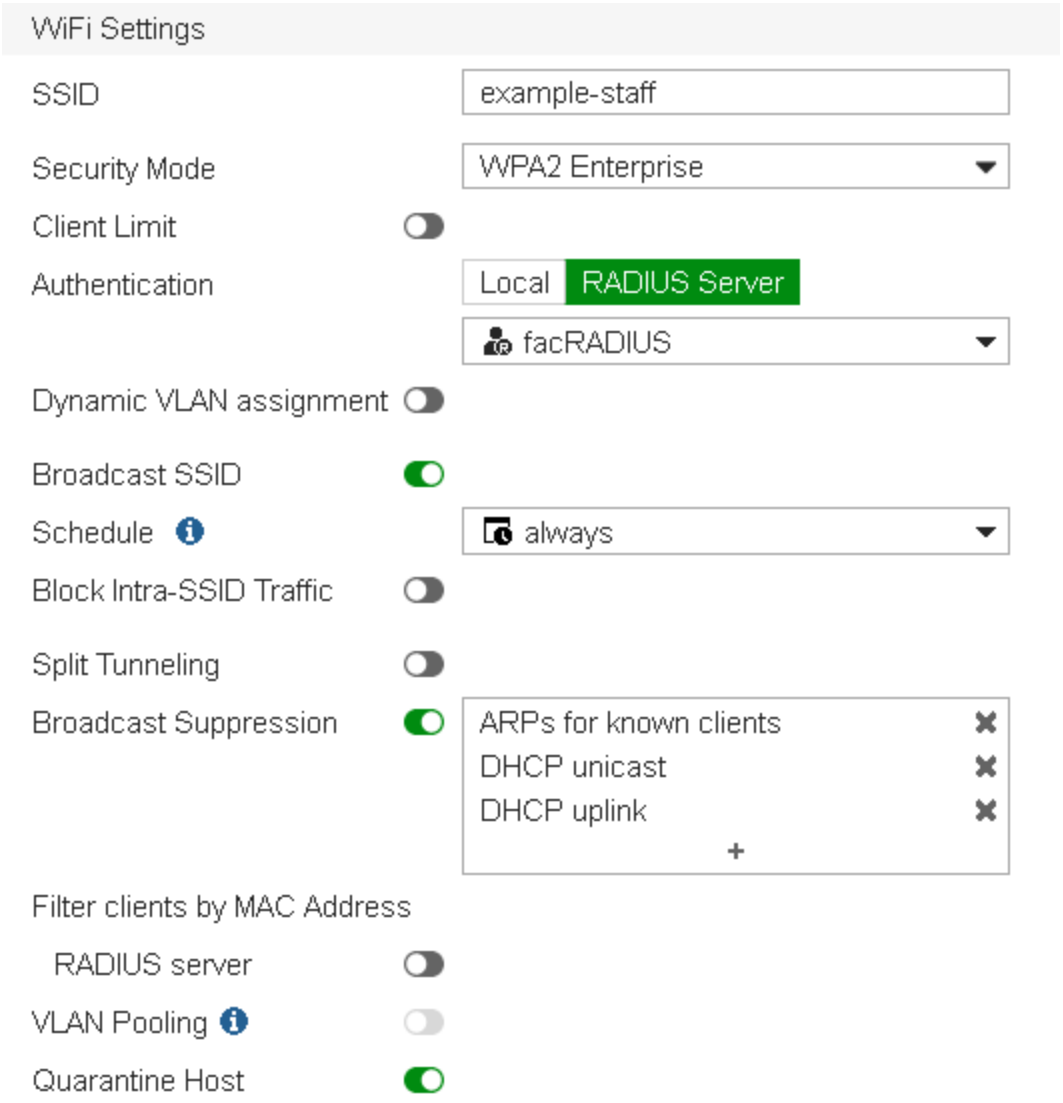
1. Go to *WiFi & Switch Controller* > *SSID* and define your wireless network.



2. Set up DHCP for your clients.



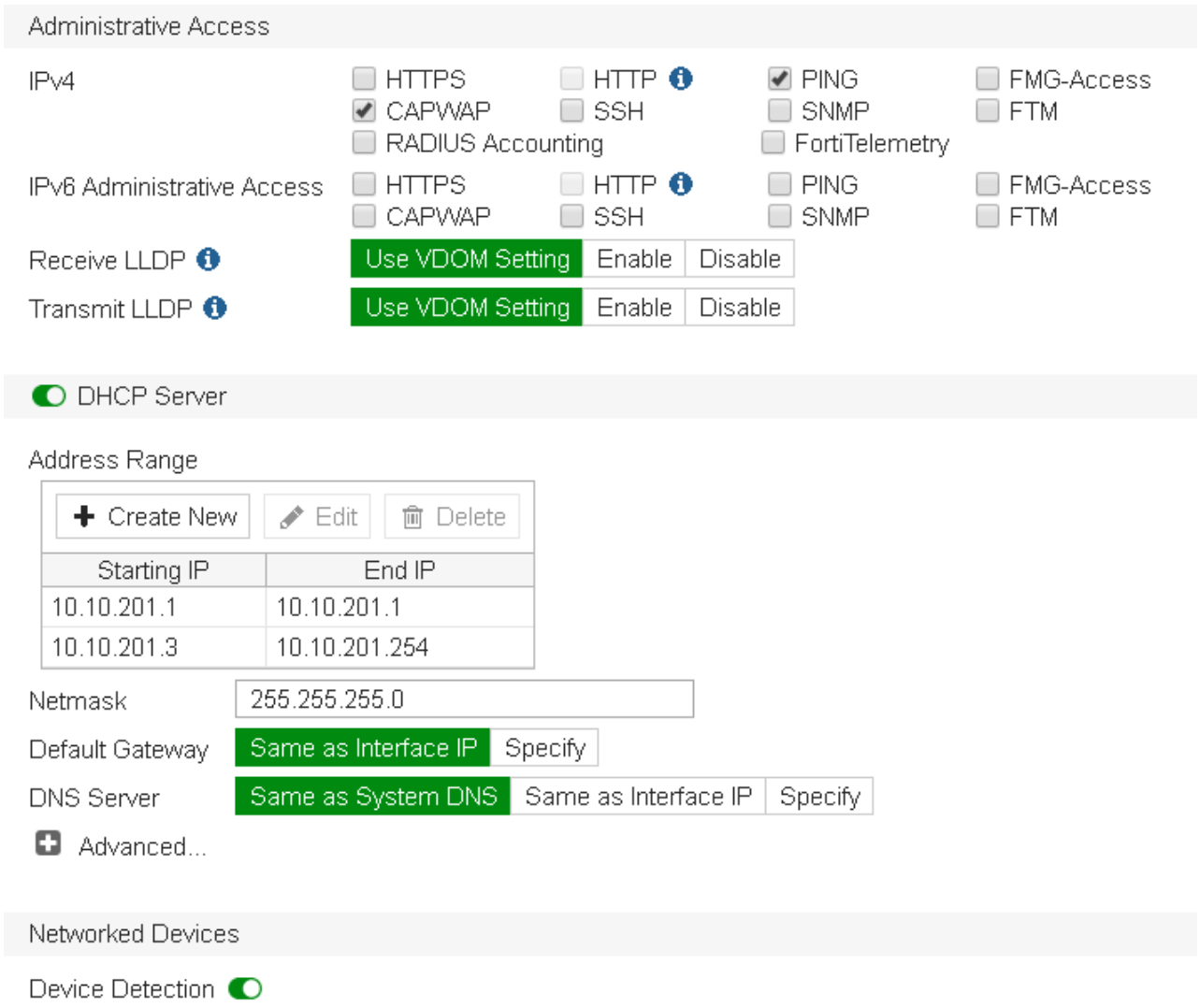
3. Configure WPA2 Enterprise security that uses the RADIUS server.



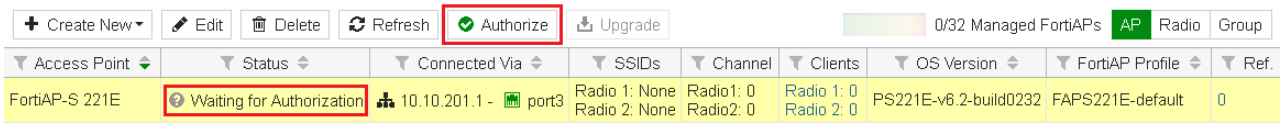
Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

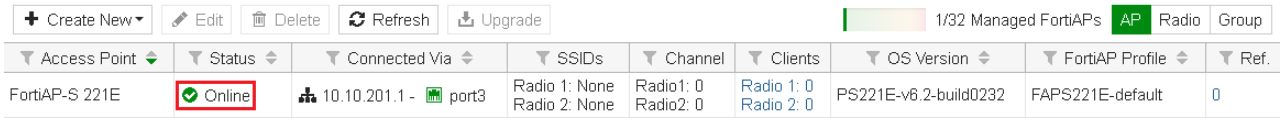
1. Go to *Network* > *Interfaces* and configure a dedicated interface for the FortiAP.
   Under *Administrative Access*, enable *PING* and *CAPWAP*, and enable *DHCP Server*.
   Under *Networked Devices*, enable *Device Detection*.



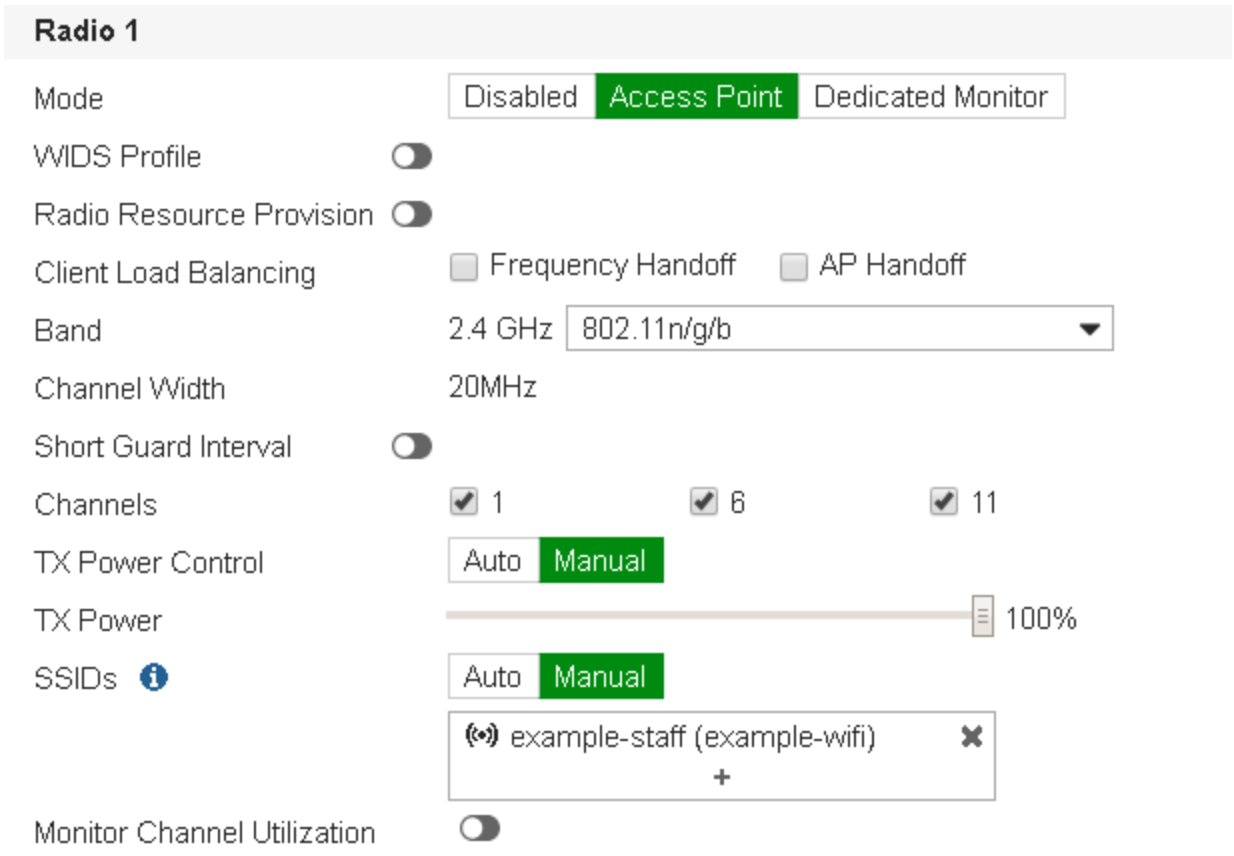
2. Connect the FortiAP unit to the interface. Then go to *WiFi & Switch Controller* > *Managed FortiAPs*. Notice the *Status* is showing *Waiting for Authorization*.
When the FortiAP is listed, select and *Authorize* it.



3. The FortiAP is now *Online*. The *Status* may take a few minutes to update.



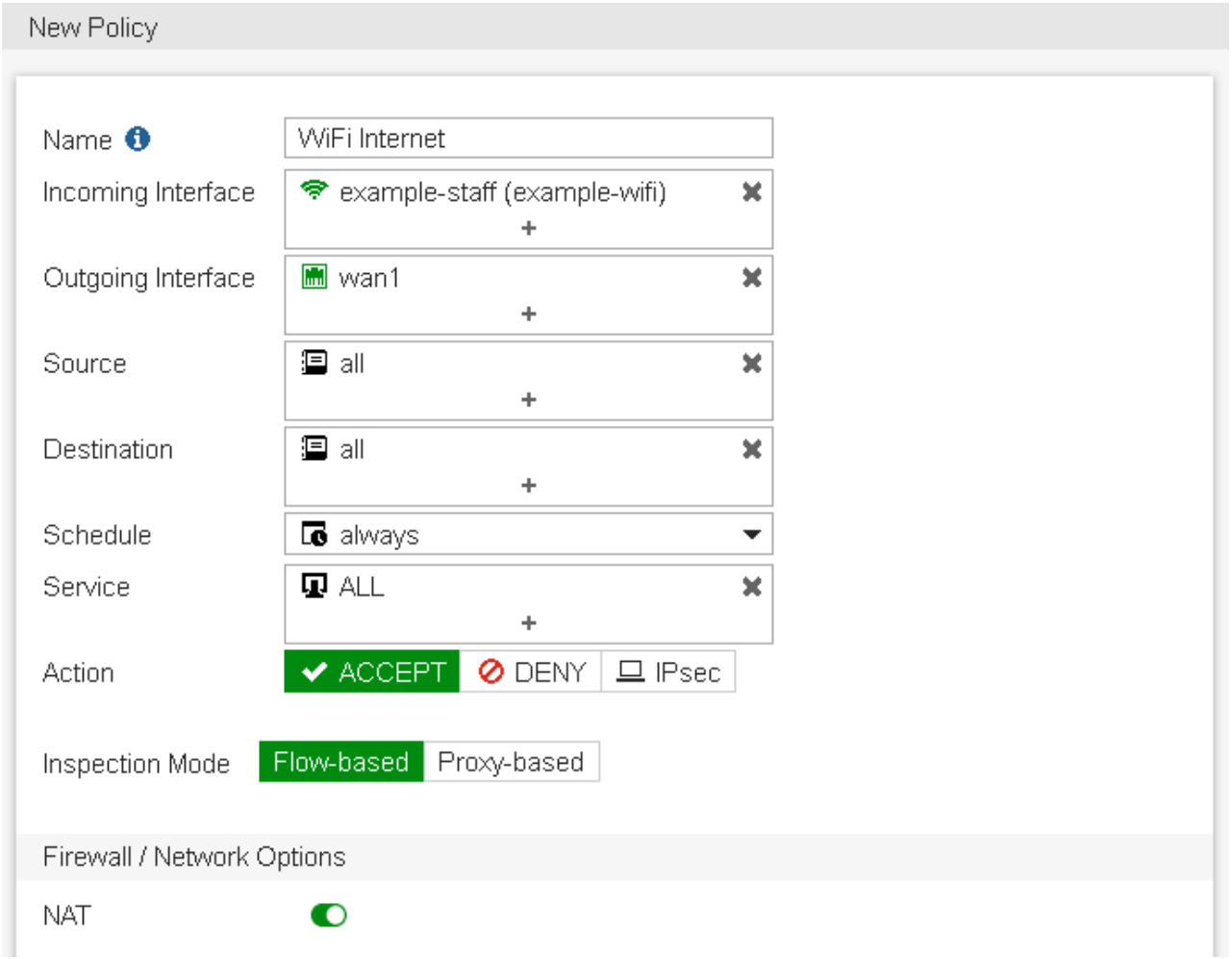
4. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and edit the profile.
This example uses a FortiAP-S 221E, so the *FAPS221E-default* profile applies.
For each radio, make sure to select your *SSID*.


Radio 1
Mode
Disabled
Access Point
Dedicated Monitor
WIDS Profile
Radio Resource Provision
Client Load Balancing
Frequency Handoff
AP Handoff
Band
2.4 GHz
802.11n/g/b
Channel Width
20MHz
Short Guard Interval
Channels
1
6
11
TX Power Control
Auto
Manual
TX Power
100%
SSIDs
Auto
Manual
example-staff (example-wifi)
Monitor Channel Utilization

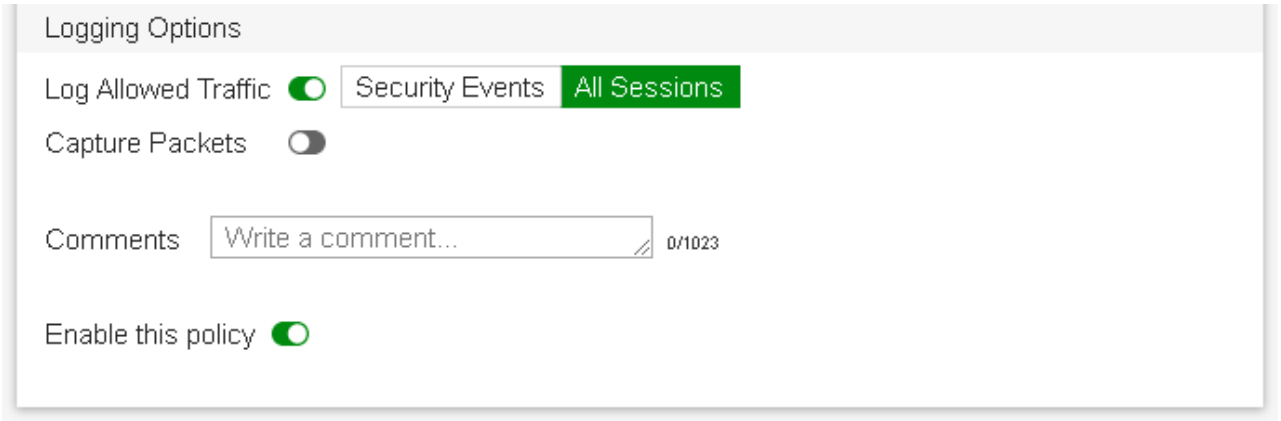
Creating the security policy

To create the security policy:

1. Go to *Policy & Objects* > *IPv4 Policy* and add a policy that allows WiFi users to access the Internet.

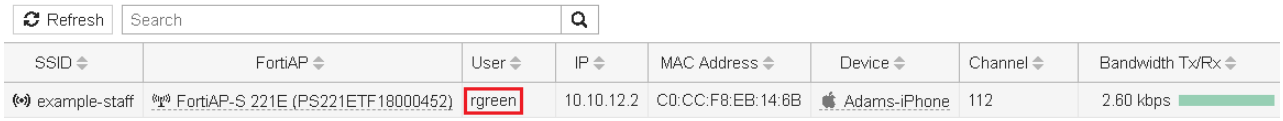


2. Under *Logging Options*, enable *Log Allowed Traffic* and *All Sessions*.

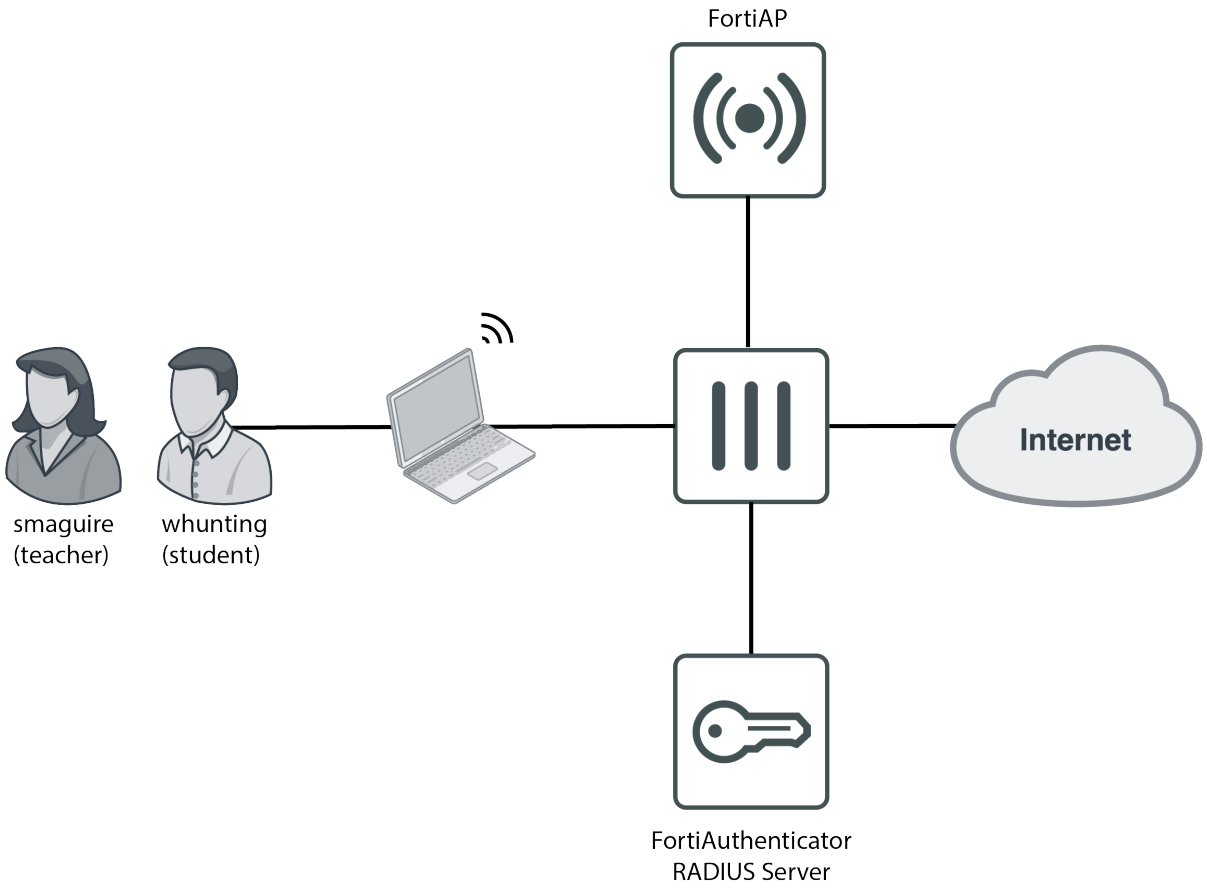


Results

1. Connect to the *example-staff* network and browse Internet sites.
   On the FortiGate, go to *Monitor* > *WiFi Client Monitor* to see that clients connect and authenticate.



WiFi with WSSO using FortiAuthenticator RADIUS and Attributes



This is an example of wireless single sign-on (WSSO) with a FortiGate and FortiAuthenticator. The WiFi users are teachers and students at a school. These users each belong to a user group, either *teachers* (*smaguire*) or *students* (*whunting*). The FortiAuthenticator performs user authentication and passes the user group name to the FortiGate so that the appropriate security policy is applied.

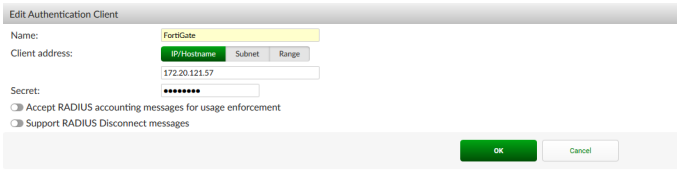
This recipe assumes that an SSID and a FortiAP are configured on the FortiGate unit. In this configuration, you will be changing the existing SSID's WiFi settings so authentication is provided by the RADIUS server.

For this example, the student security policy applies a more restrictive web filter.

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

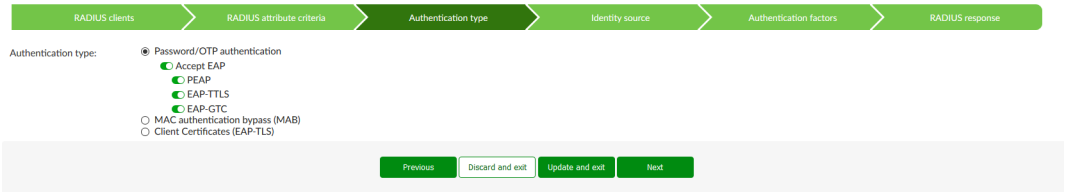
To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.



To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable all *EAP* types.

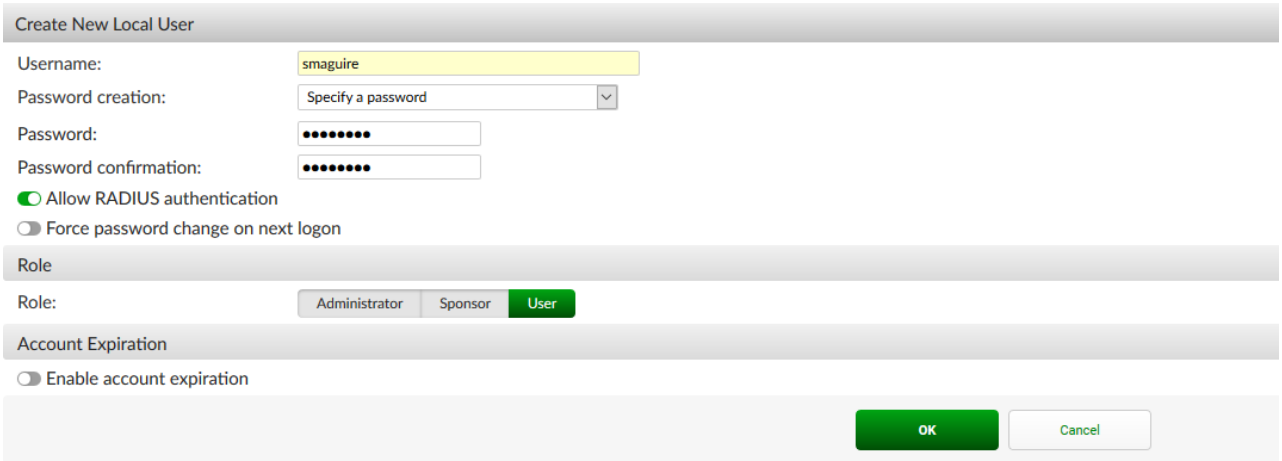


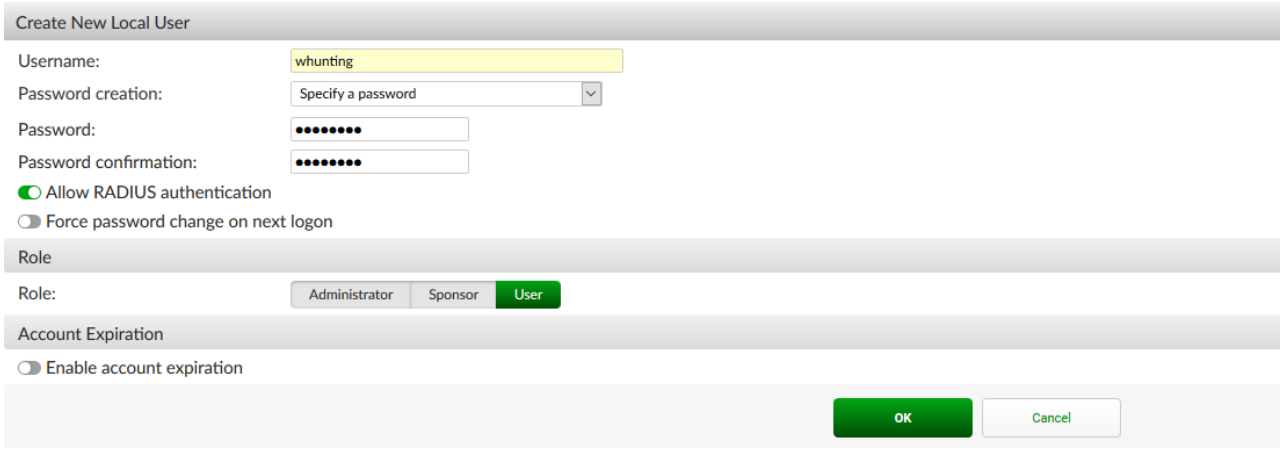
5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
6. Review the remaining configurations, and click *Save and Exit*.

Creating users on the FortiAuthenticator

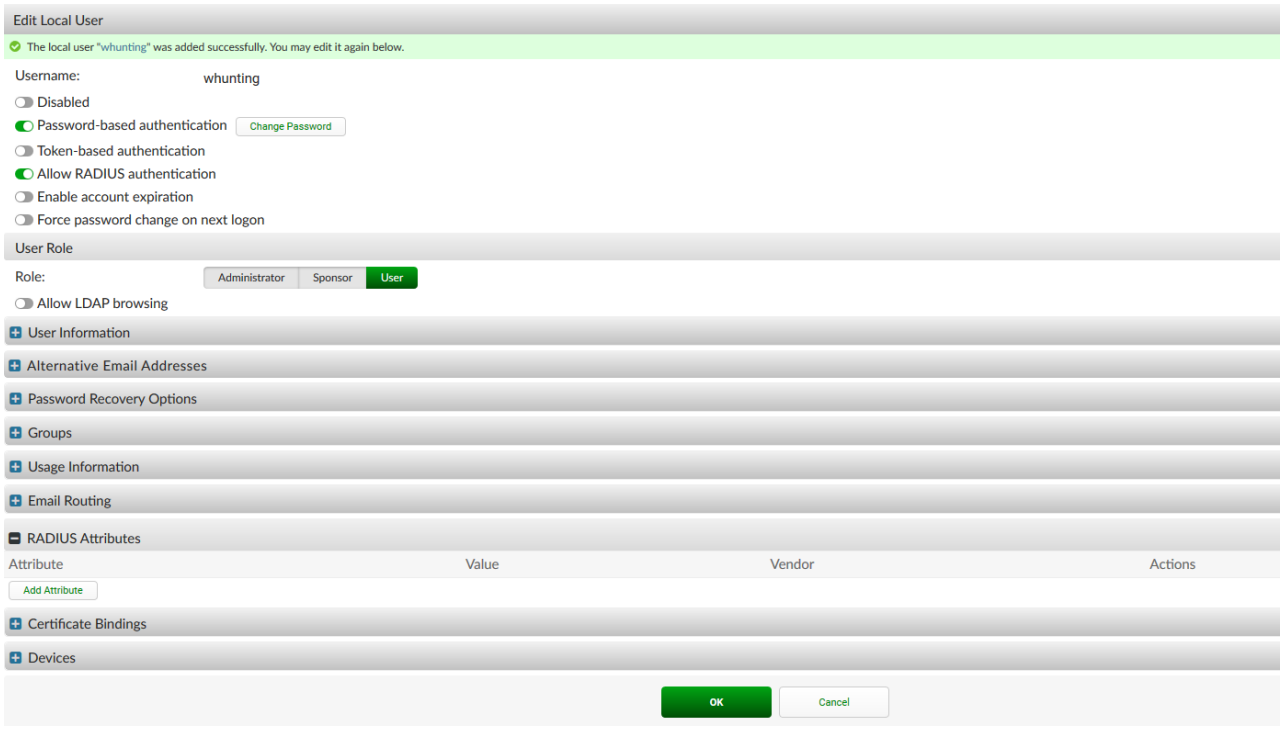
To create users:

1. Go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
   Create one teacher user (*smaguire*) and another student user (*whunting*).





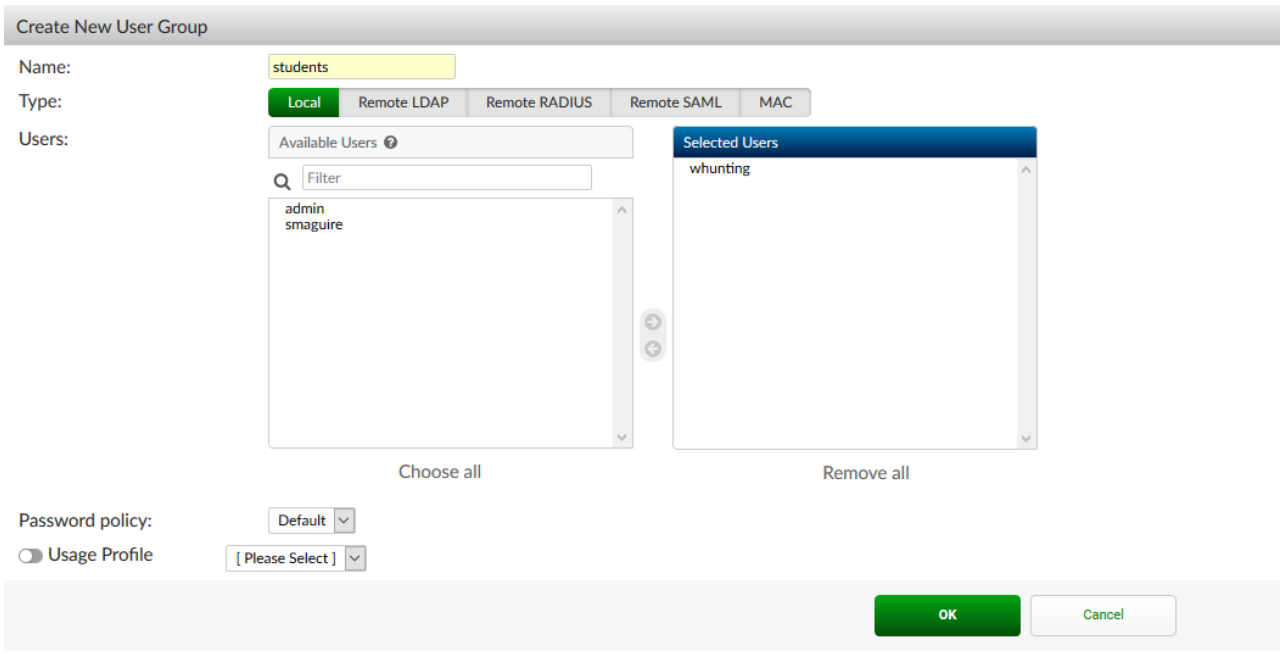
2. Note that, after you create the users, *RADIUS Attributes* appears as an option.
   If your configuration involves multiple users, it is more efficient to add RADIUS attributes in their respective user groups, in the next step.



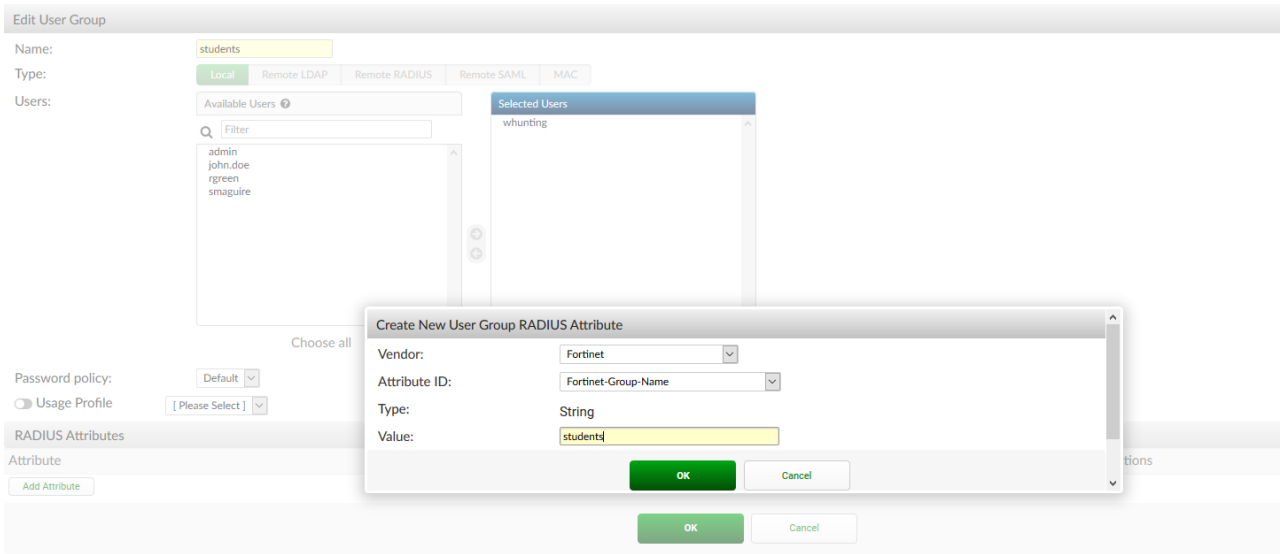
Creating user groups on the FortiAuthenticator

To create user groups:

1. Go to *Authentication* > *User Management* > *User Groups* and create two user groups: *teachers* and *students*.
   Add the users to their respective groups.



2. Once created, edit both user groups and select *Add Attribute*.
3. Add the *Fortinet-Group-Name* RADIUS attribute to each group, which specifies the user group name to be sent to the FortiGate.

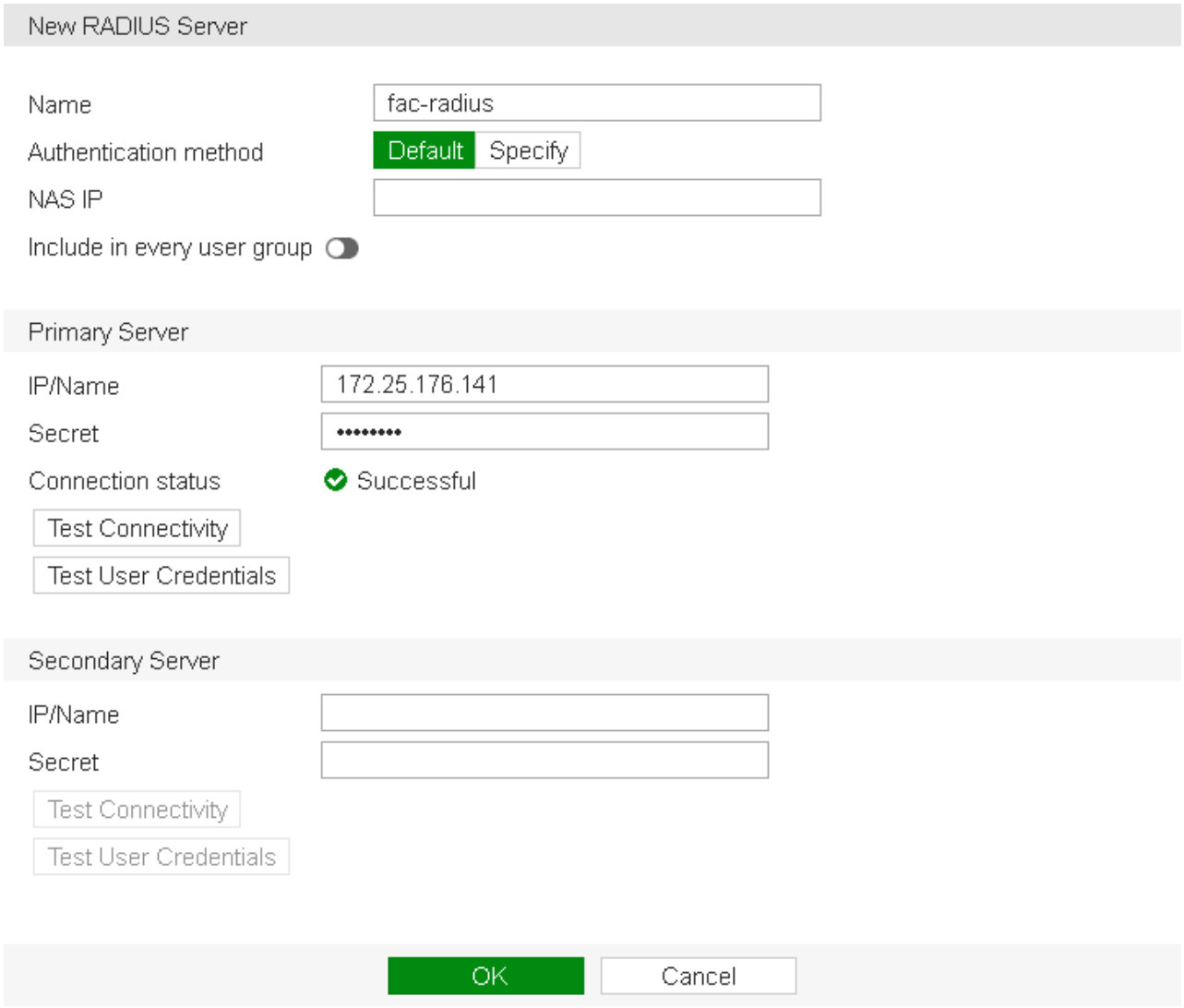


Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server

To configure the FortiGate to use the FortiAuthenticator RADIUS server:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*.
   Enter a *Name*, the Internet-facing IP address of the FortiAuthenticator, and enter the same *Primary Server Secret* entered on the FortiAuthenticator.

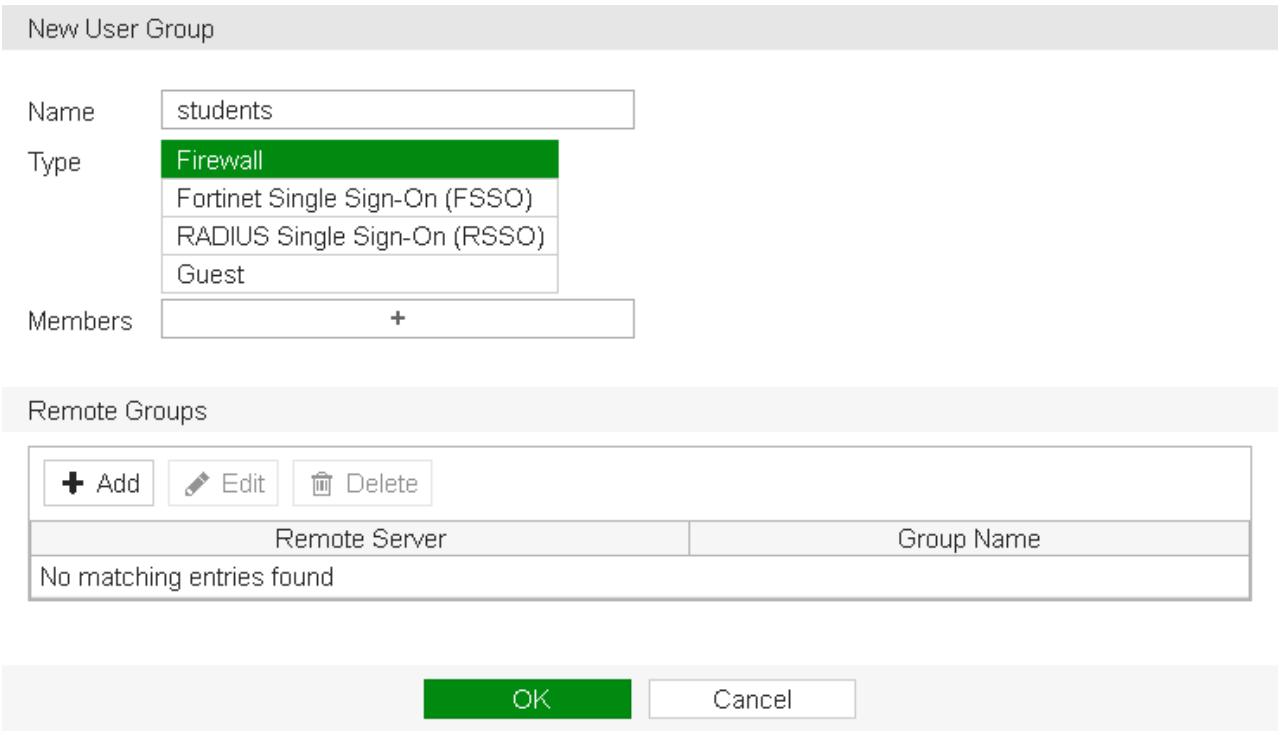
Select *Test Connectivity* to confirm the successful connection.



Configuring user groups on the FortiGate

To configure user groups on the FortiGate:

1. Go to *User & Device* > *User Groups* and create two groups named the same as the ones created on the FortiAuthenticator.



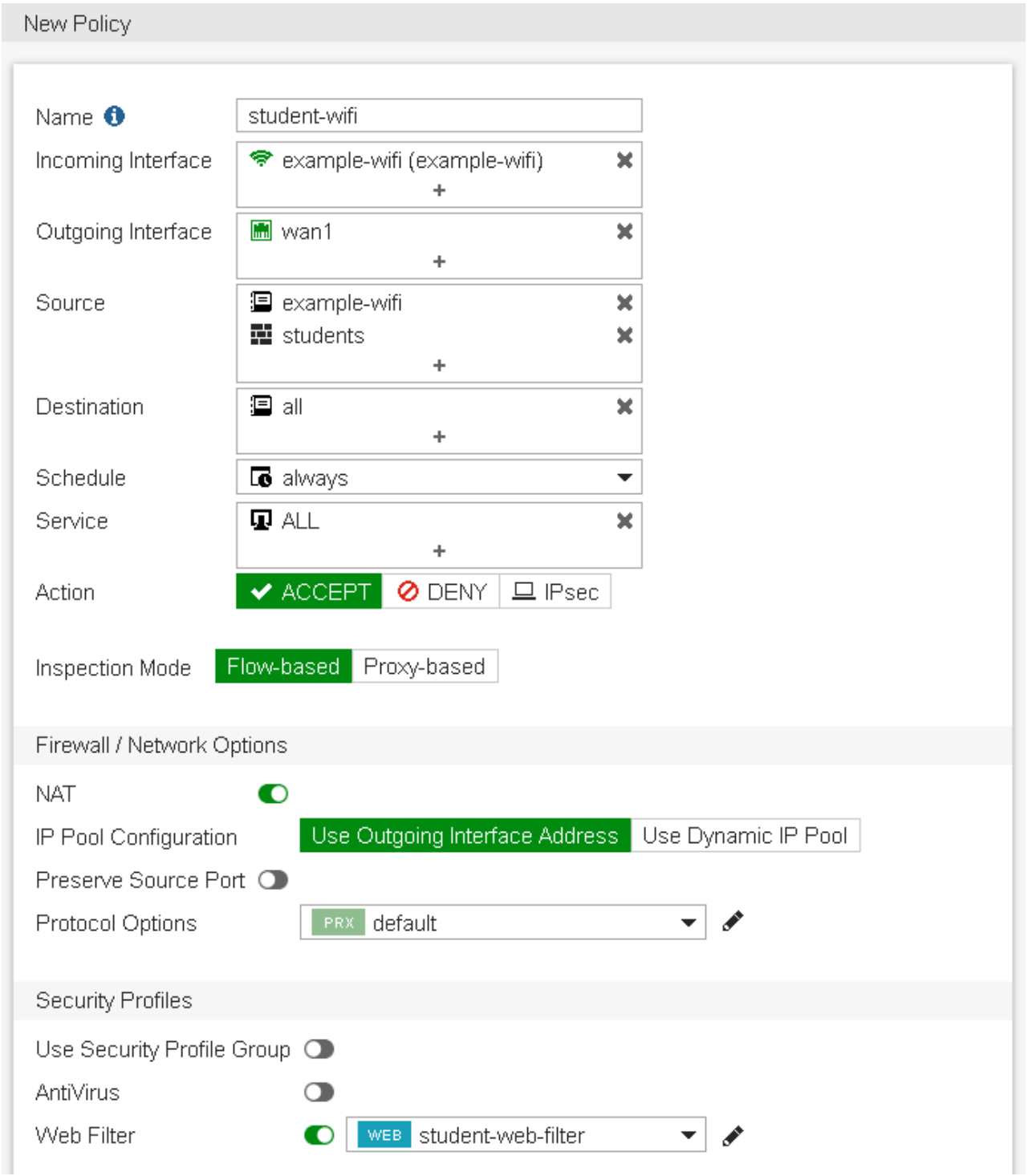
Do not add any members to either group.

Creating security policies

To create a security policy:

1. Go to *Policy & Objects* > *IPv4 Policy* and select *Create New*.
   Create two policies (*student-wifi* and *teacher-wifi*) with WiFi-to-Internet access: one policy with *Source* set to the *students* user group, and the other set to *teachers*. Make sure to add the SSID address (*example-wifi*) to both policies also.

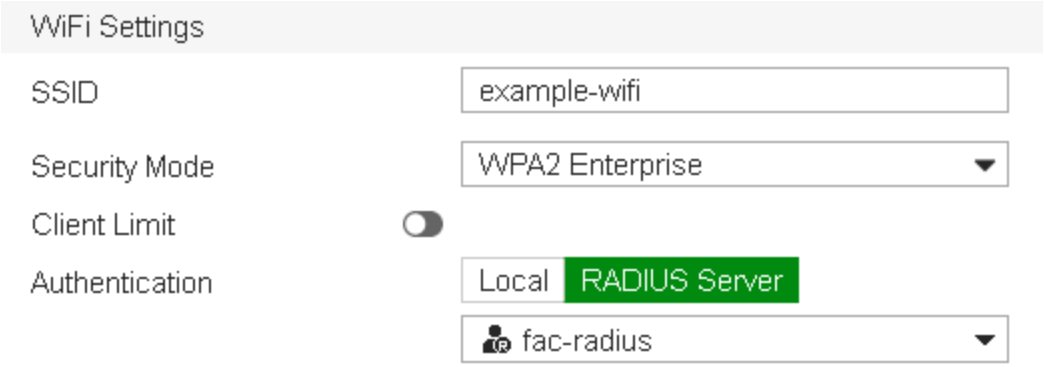
The student policy has a more restrictive *Web Filter* profile enabled.



Configuring the SSID to RADIUS authentication

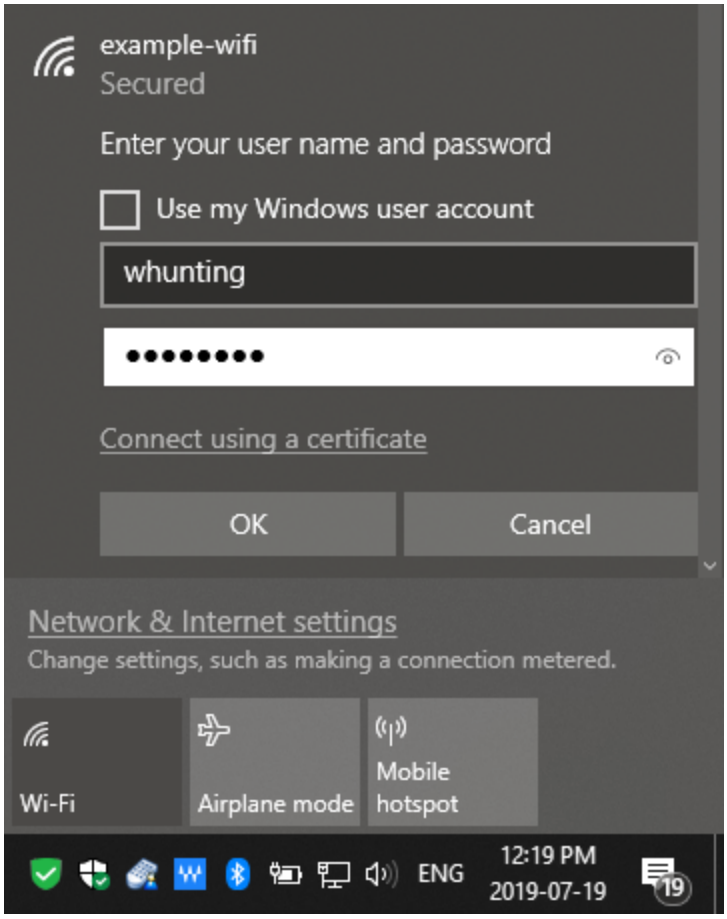
To configure the SSID to RADIUS authentication:

1. Go to *WiFi & Switch Controller* > *SSID* and edit your pre-existing SSID interface.
   Under *WiFi Settings*, set *Security Mode* to *WPA2 Enterprise*, set *Authentication* to *RADIUS Server*, and add the RADIUS server configured on the FortiGate earlier from the dropdown menu.

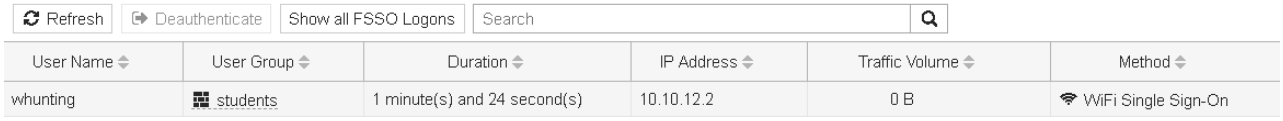


Results

1. Connect to the WiFi network as a student.



2. Then on the FortiGate go to *Monitor* > *Firewall User Monitor*. From here you can verify the user, the user group, and that the WSSO authentication method was used.



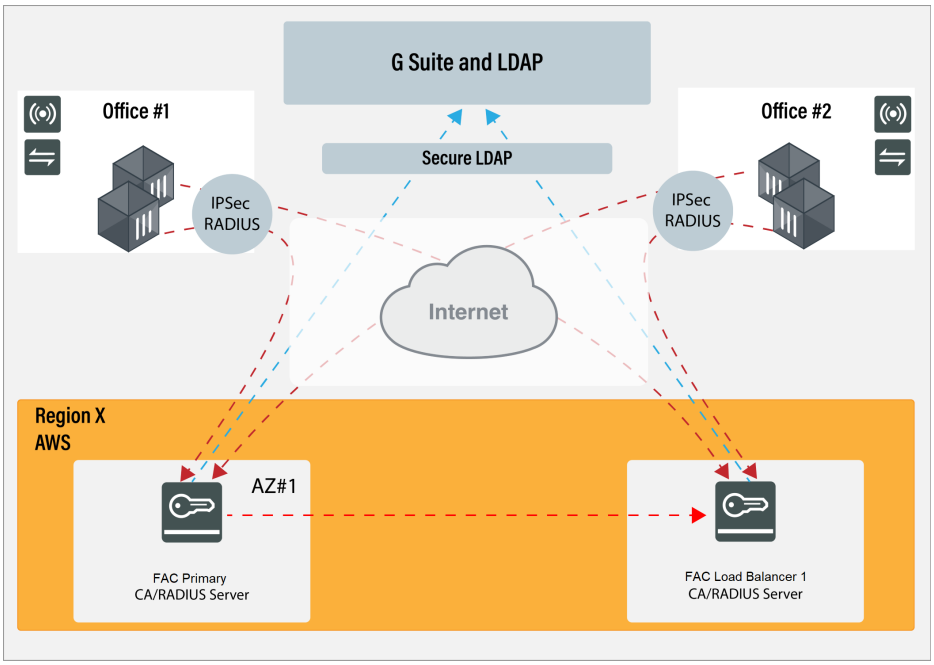
LDAP Authentication

This section describes configuring LDAP authentication.

G Suite integration using LDAP

This article explains how to integrate the FortiAuthenticator with G Suite Secure LDAP using client authentication through a certificate. You will use the LDAP in Google DB to authenticate end users for 802.1X and VPN.

1. Generating the G Suite certificate on page 146
2. Importing the certificate to FortiAuthenticator on page 148
3. Configuring LDAP on the FortiAuthenticator on page 148
4. Troubleshooting on page 150



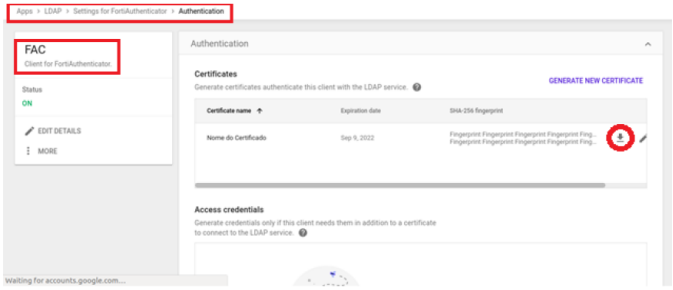
Generating the G Suite certificate

You must first generate certificates to authenticate the LDAP client with Secure LDAP service.

To generate certificate authentication:

1. From the Google Admin console, go to *Apps* > *LDAP*.
2. Select one of the clients in the list.
3. Click the *Authentication* card.
4. Click *GENERATE NEW CERTIFICATE*, then click the download icon to download the certificate.

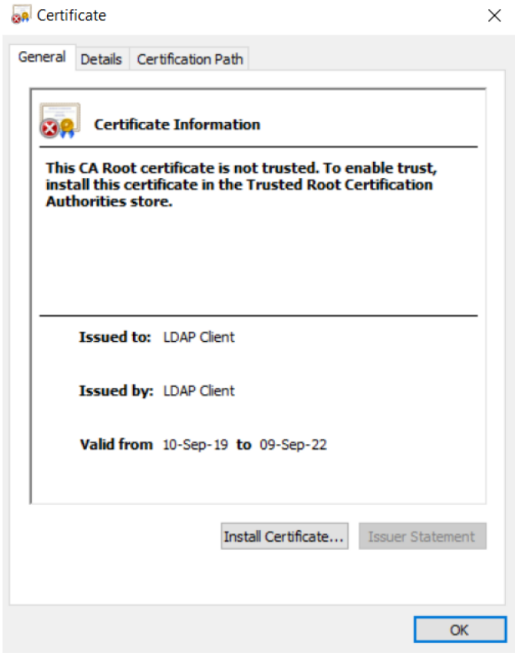
5. Upload the certificate to your client, and configure the application.
   Depending on the type of LDAP client, configuration may require LDAP access credentials. See Generate access credentials.



Once you have uploaded the certificate to your client, G Suite will generate a client certificate and key.

Example:

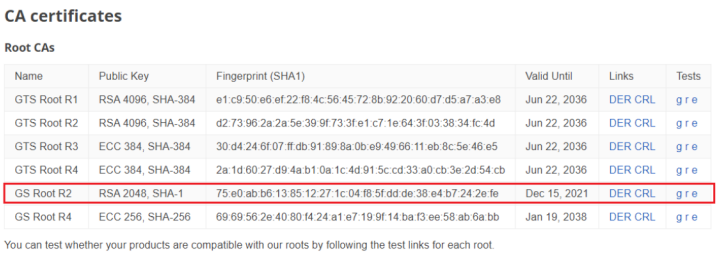
- Cert: `Google_2022_09_09_72372.crt`
- Key: `Google_2022_09_09_72372.key`



Store the certificate and key in a safe place.

By default, FortiAuthenticator will not trust the certificate issued by Google. You must install a Google Trusted CA to match the chain group, which can be downloaded at https://pki.goog/.

- `GS Root R2`



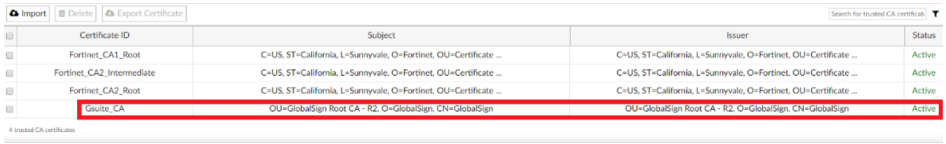
Importing the certificate to FortiAuthenticator

This series of steps can be performed on the primary FortiAuthenticator.

To import the trusted CA certificate:

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* > *Import*.
2. Enter a Certificate ID, upload a file, and click *OK*.

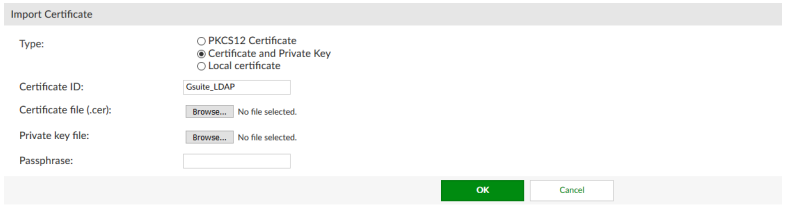
Results:



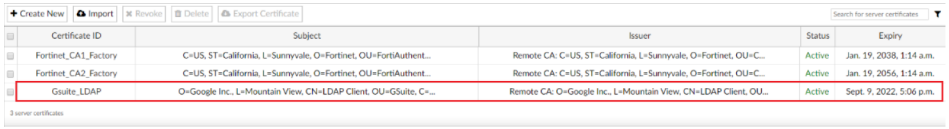
You can now import the LDAP certificate generated by G Suite.

To import the client authentication certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services* > *Import*.
2. Select *Certificate and Private Key* as the *Type*.
3. Enter the Certificate ID, choose the files for the previously saved certificate and private key files, and select *OK*.
4.



Results:

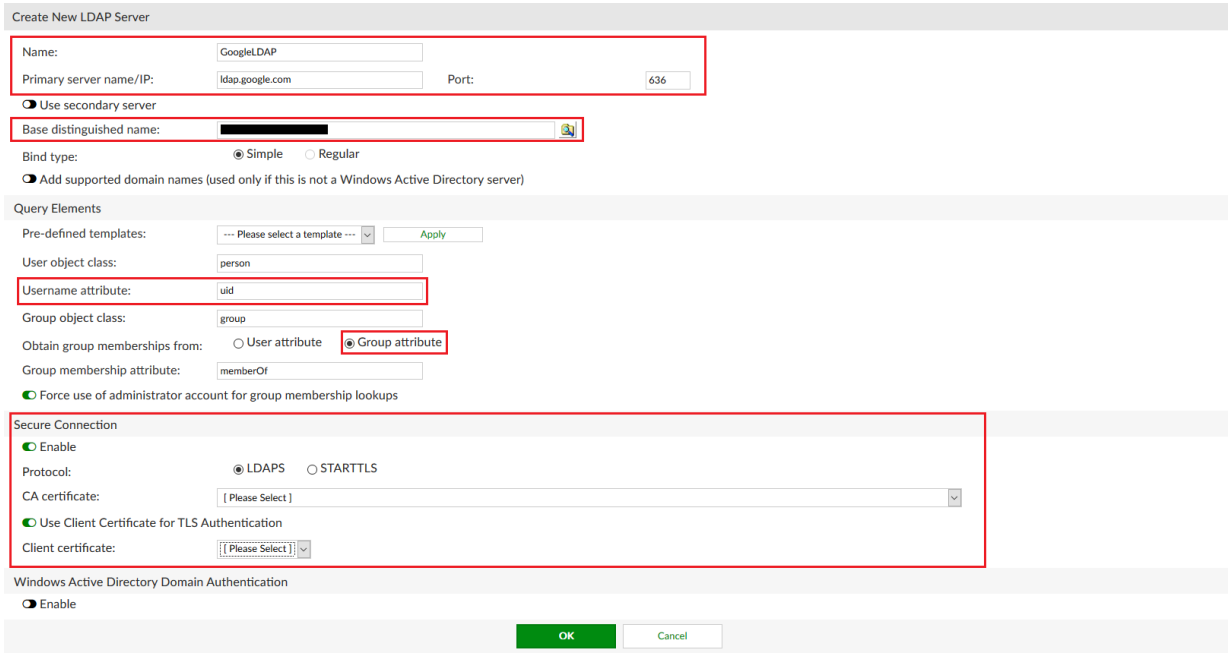


Configuring LDAP on the FortiAuthenticator

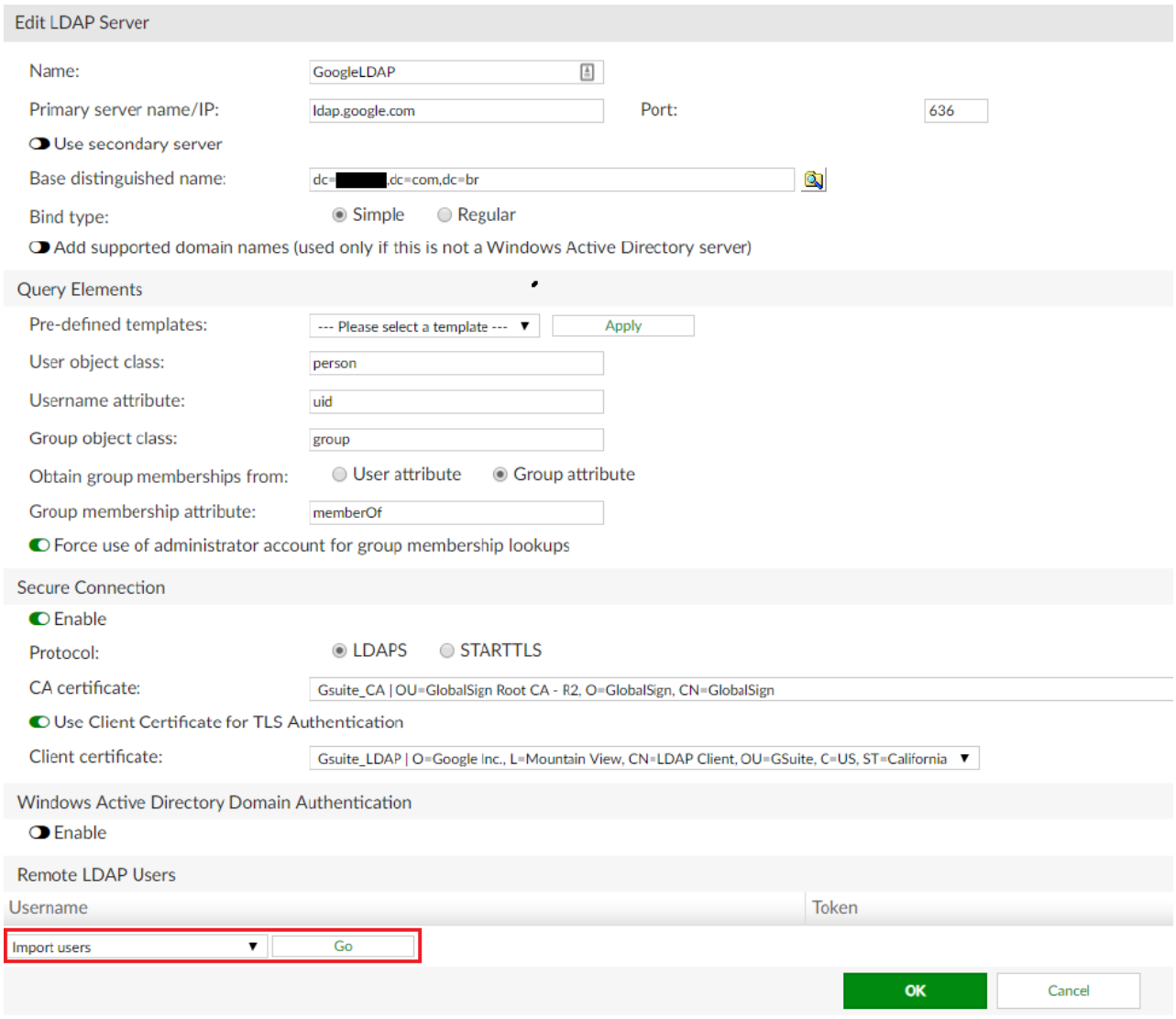
Now you can finish the LDAPS configuration using client authentication through certificate.

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* > *Create New*, and enter the following information:
   a. Enter a name.
   b. For *Primary server name/IP* enter `ldap.google.com`, and set the port to `636`.
   c. Enter the base distinguished name.
   d. For the Username attribute, enter `uid`.
   e. Select the option to obtain group memberships from *Group attribute*.
   f. Enable *Secure Connection* and select either *LDAPS* or *STARTTLS* as the Protocol, and select the Google CA certificate.

g. Enable *Use Client Certificate for TLS Authentication,* and select the LDAP certificate.



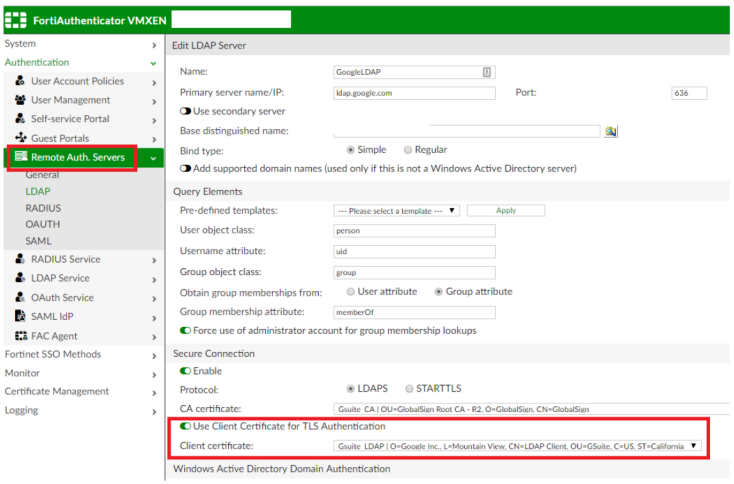
2. Select *OK*.
If required, you can now import users by clicking the *Go* button next to the *Import users* dropdown. This is not a required step, but can be done in cases where you want to include additional information to their accounts or assign FortiTokens.



Troubleshooting

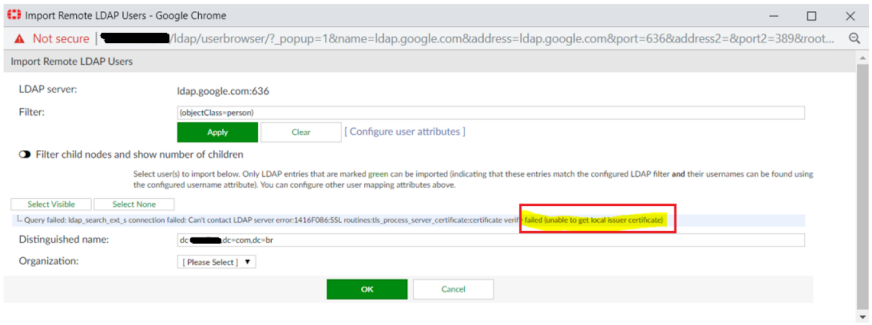
Missing option to use client certificate for TLS authentication

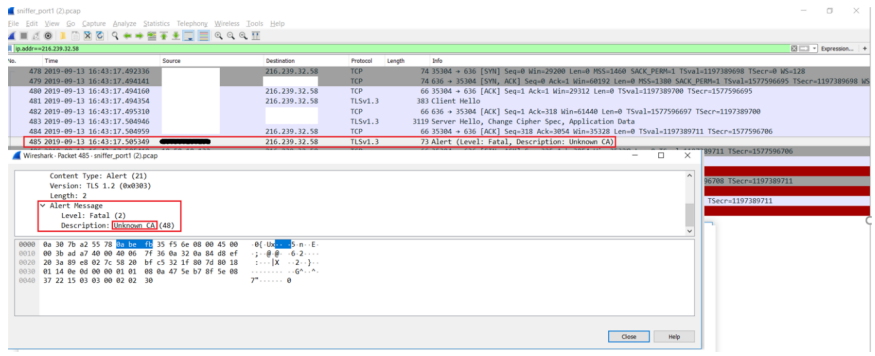
Use Client Certificate for TLS Authentication is only supported in FortiAuthenticator 6.0.1 and higher.



Certificate error messages

The following is an example of an incorrect Trusted CA certificate entry. Please verify that you have followed the steps included in Generating the G Suite certificate on page 146.





SAML Authentication

This section describes configuring SAML authentication.

SAML IdP proxy for Azure

This recipe describes how to set up FortiAuthenticator as a SAML IdP proxy for Microsoft Azure.

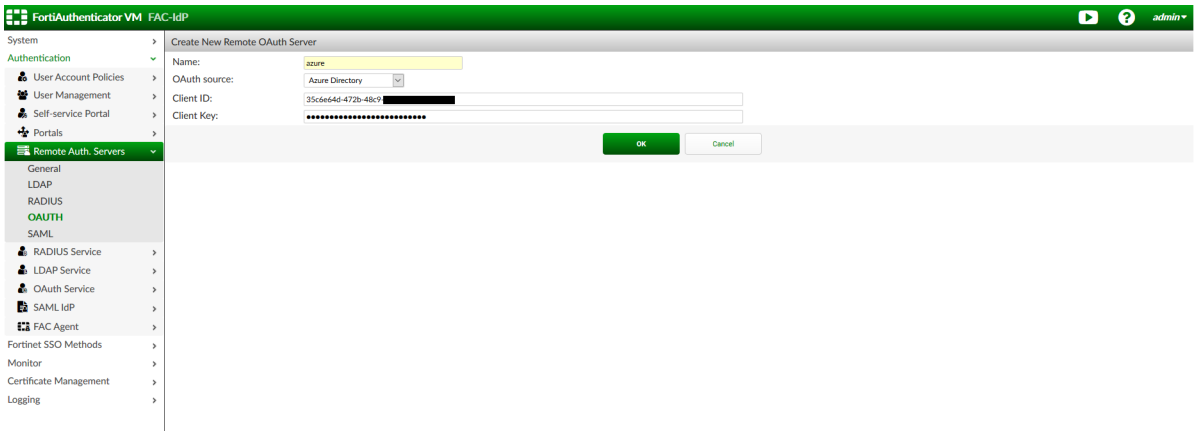
To configure FortiAuthenticator as a SAML IdP proxy for Azure:

1. Configuring OAuth settings on page 152
2. Configuring the remote SAML server on page 153
3. Enabling the SAML SP FSSO Portal on page 153
4. Configuring an Azure realm on page 154
5. Configuring SAML IdP settings on page 154
6. Configuring the login page replacement message on page 155
7. Results on page 156

Configuring OAuth settings

To configure remote OAuth settings:

1. On FortiAuthenticator, go to *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Provide a name for the server and select *Azure Directory* as the OAuth source.
3. Enter the client ID and client key from the SAML application on your Azure account.

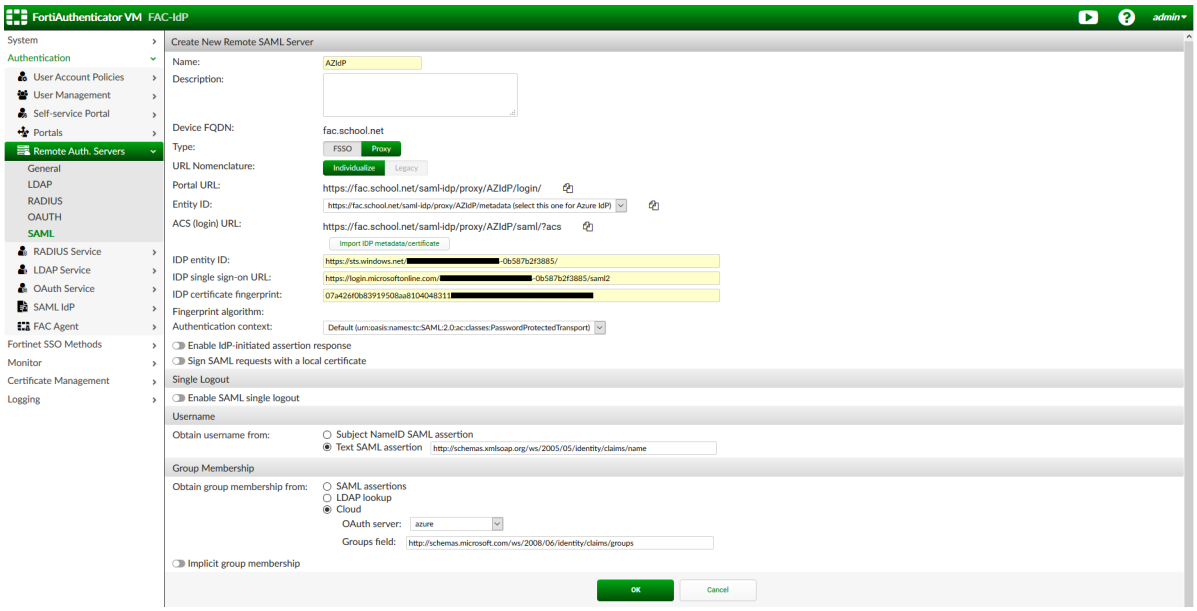


4. Click *OK* to save your changes.

Configuring the remote SAML server

To configure the remote SAML server:

1. Go to *Remote Auth. Servers* > *SAML*, and click *Create New*.
   The server name must match the one created in https://portal.azure.com/. For example, if the name in Azure is set as AZIdP, the SAML server should also use AZIdP (case sensitive).
2. For the *Entity ID*, click the dropdown menu and select the Azure IdP option.
3. Import the IdP metadata from Azure. To download and import the Azure federation metadata:
   a. In Azure, go to *Azure Active Directory* > *App Registrations* and select the application being used for SAML authentications for your FortiAuthenticator.
   b. In *Endpoints*, select the federation metadata document, enter the URL into the browser, and save it as an XML file.
   c. Click *Import IDP metadata/certificate*, and upload the federation metadata file.
4. In Group Membership, select *Cloud* and choose the previously created Azure OAuth server.
5. At the top of the page, select *Proxy* as the Type, and copy the *Portal URL* to be used later when customizing the replacement message.



6. Click *OK* to save your changes.

Enabling the SAML SP FSSO Portal

To enable the SAML SP FSSO Portal:

1. Go to *Fortinet FSSO Methods* > *SSO* > *Portal Services* and enable the SAML portal.
2. Go to *Fortinet FSSO Methods* > *SSO* > *SAML Authentication* and create a new SAML server.
   Select the previously created remote SAML server and click *OK*.

Configuring an Azure realm

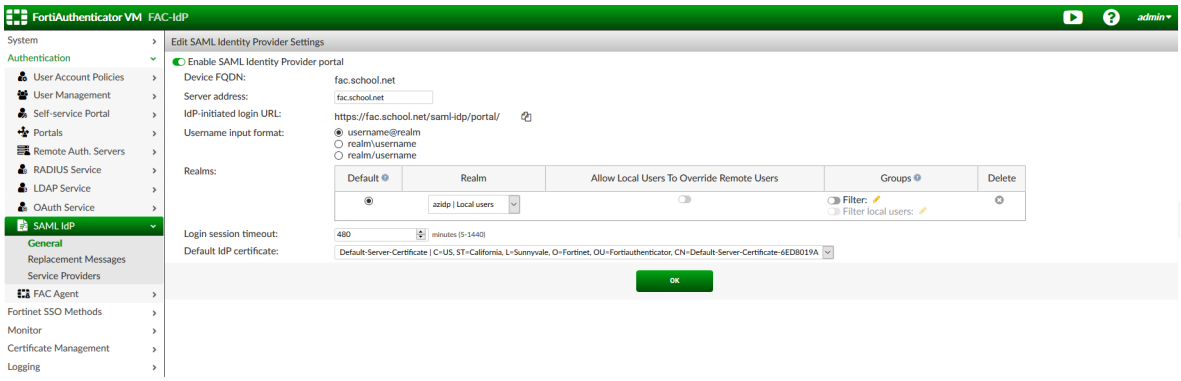
To create an Azure realm and add it to the IdP:

1. Go to *Authentication* > *User Management* > *Realms*
2. Click *Create New*.
3. Add the details of the Azure realm, and click *OK*.

Configuring SAML IdP settings

To configure general settings:

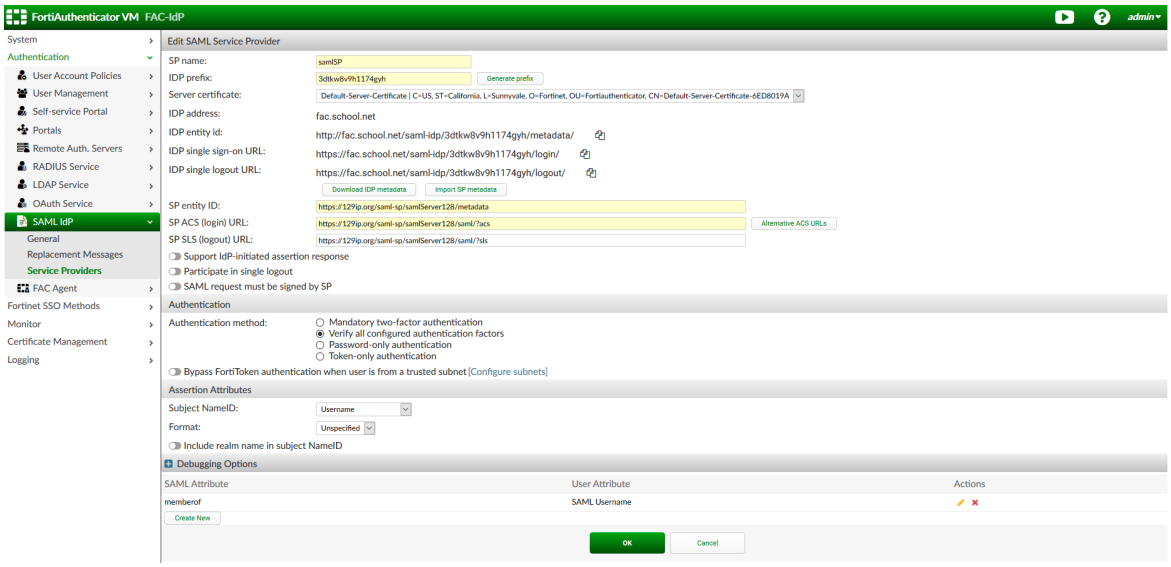
1. Go to *Authentication* > *SAML IdP* > *General.*
2. Enable the SAML identity provider portal and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Realms**: Add the realm associated with the remote server for Azure IdP.
   c. **Default IdP certificate**: Select a default certificate to use.



3. Click *OK* to save your changes.

To configure service provider settings:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
   The name can be anything you want.
2. Enter the SP information from the client you will be using as the SAML service provider.
3. Download the IdP metadata.
   This can be used to set up the SAML IdP configuration in your SAML SP client (if allowed by your client).
4. Under *SAML Attribute* click *Create New*, and enter a *SAML Attribute* name that your SAML SP is expecting to identify the user. Select a *User Attribute* for this selection. If you're unsure of which attribute to pick, select *SAML Username*.

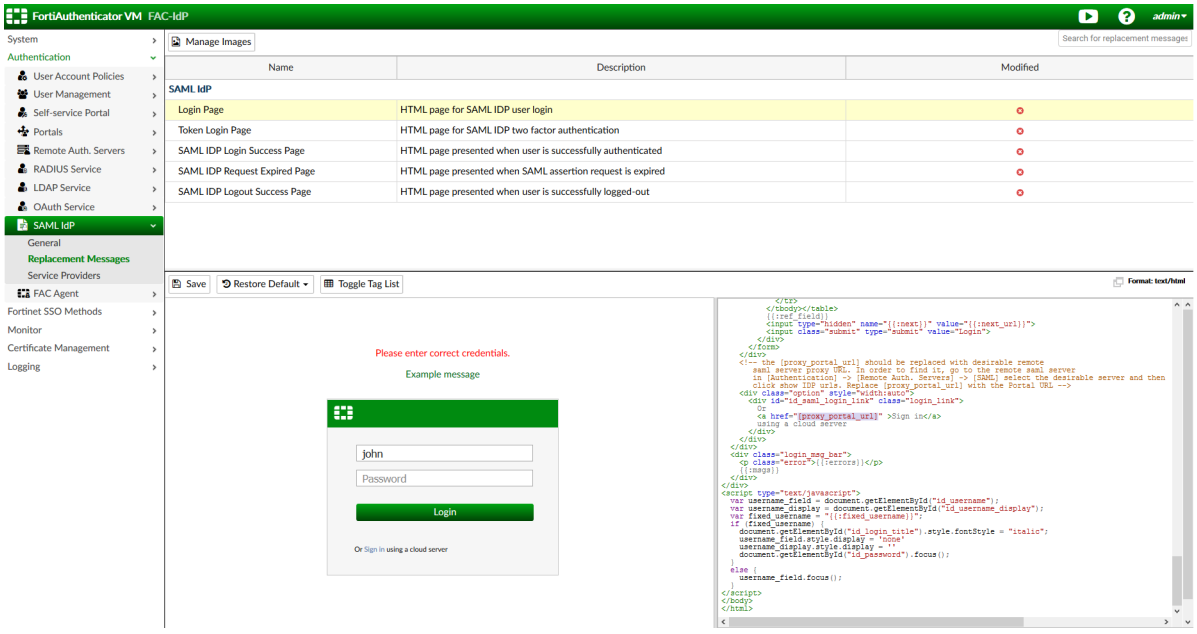


5. Click *OK* to save your changes.

Configuring the login page replacement message

To configure the login page replacement message:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*.
2. On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
3. In the text/html editor, scroll down until you see the `[proxy_portal_url]` placeholder and replace it with the previously saved proxy portal URL.



4. Click *Save*.

Results

To test Azure login through the SP:

1. Enter in the portal login URL from the service provider in a new browser.
   You are redirect you to the FAC's IdP-server and proxy page.
2. Click on the link below the login options to be redirected to Microsoft's login page.

SAML IdP proxy for G Suite

This recipe describes how to set up FortiAuthenticator as a SAML IdP proxy for Google G Suite.

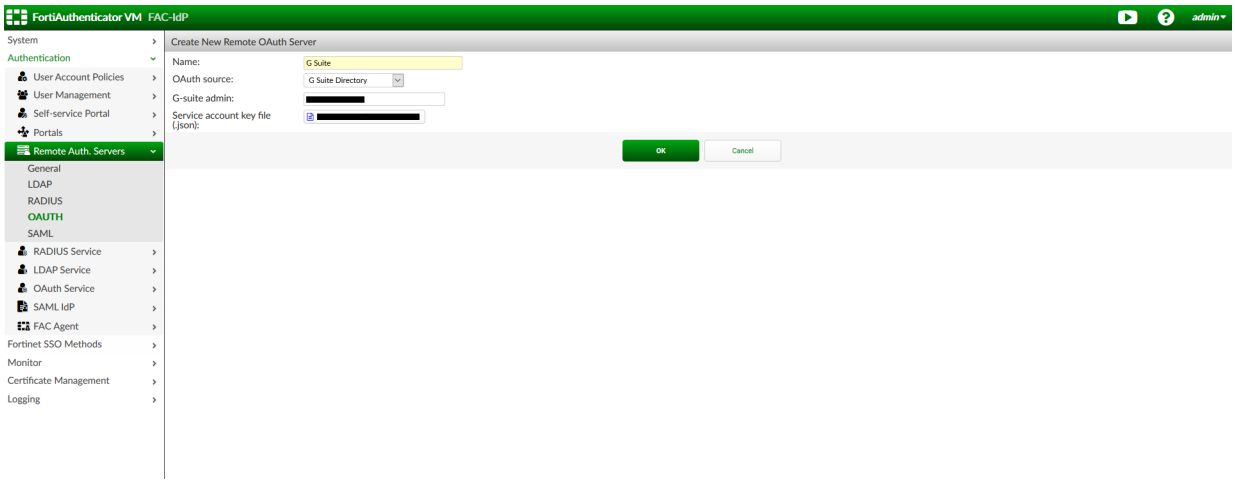
To configure FortiAuthenticator as a SAML IdP proxy for G Suite:

1. Configuring OAuth settings on page 156
2. Configuring the remote SAML server on page 157
3. Enabling the SAML SP FSSO Portal on page 157
4. Configuring a G Suite Realm on page 158
5. Configuring IdP settings on page 158
6. Configuring the login page replacement message on page 159
7. Results on page 160

Configuring OAuth settings

To configure remote OAuth settings:

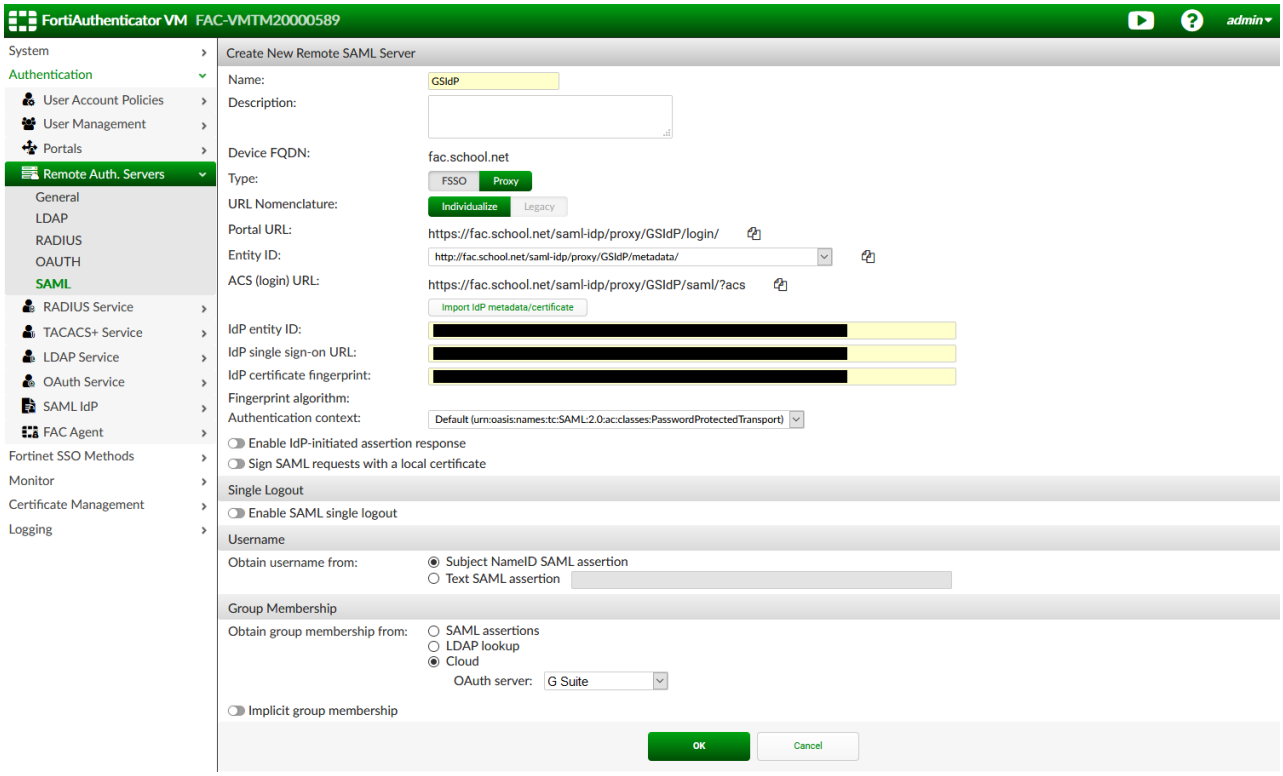
1. On FortiAuthenticator, go to *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Provide a name for the server and select *G Suite Directory* as the OAuth source.
3. Enter the *G-suite admin*, and upload the *Service account key file* from the SAML application on your G Suite account.
4. Click *OK* to save your changes.



Configuring the remote SAML server

To configure the remote SAML server:

1. Go to *Remote Auth. Servers* > *SAML*, and click *Create New*.
   The server name must match the one created in G Suite. For example, if the name in G Suite is set as GSIdP, the SAML server should also use GSIdP (case sensitive).
2. Import the IdP metadata obtained from the SAML app on G Suite.
3. In *Username*, select *Subject NameID SAML assertion*.
4. In *Group Membership*, select *Cloud* and choose the previously created G Suite OAuth server.
5. At the top of the page, select *Proxy* as the Type, and copy the *Portal URL* to be used later when customizing the replacement message.



6. Click *OK* to save your changes.

Enabling the SAML SP FSSO Portal

To enable the SAML SP FSSO Portal:

1. Go to *Fortinet FSSO Methods* > *SSO* > *Portal Services* and enable the SAML portal.
2. Go to *Fortinet FSSO Methods* > *SSO* > *SAML Authentication* and create a new SAML server.
   Select the previously created remote SAML server and click *OK*.

Configuring a G Suite Realm

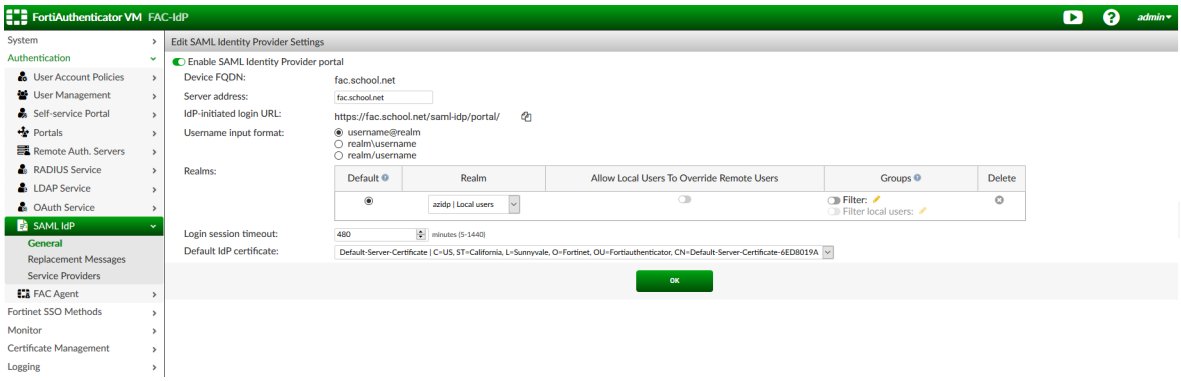
To create a G Suite Realm and add it to the IdP:

1. Go to *Authentication* > *User Management* > *Realms.*
2. Click *Create New*.
3. Add the details of the G Suite realm, and click *OK*.

Configuring IdP settings

To configure general settings:

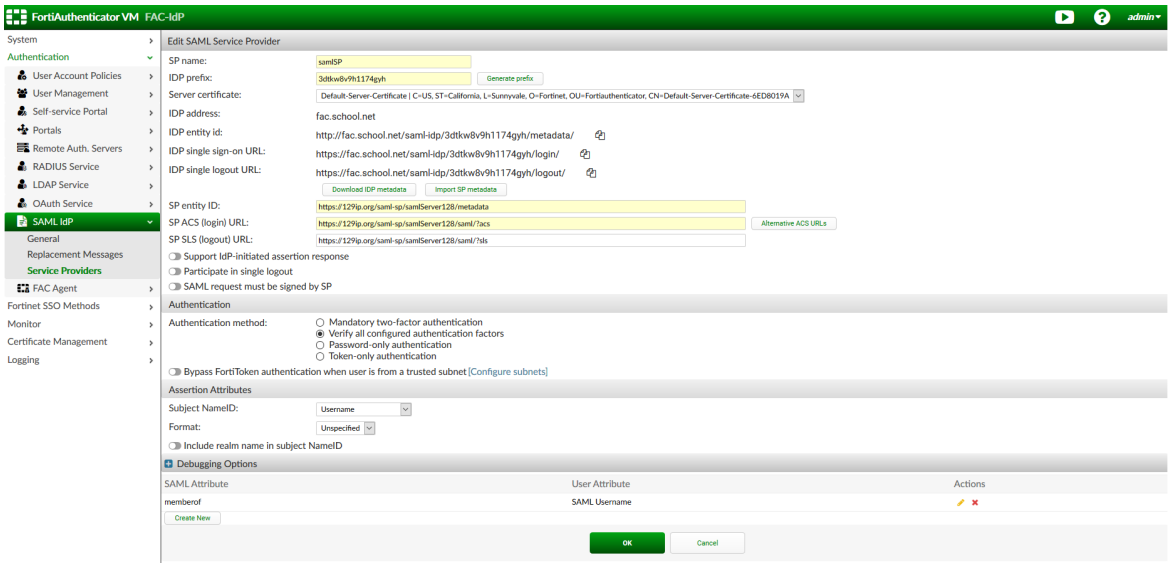
1. Go to *Authentication* > *SAML IdP* > *General.*
2. Enable the SAML identity provider portal and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Realms**: Add the realm associated with the remote server for G Suite.
   c. **Default IdP certificate**: Select a default certificate to use.



3. Click *OK* to save your changes.

To configure service provider settings:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
   The name can be anything you want.
2. Enter the SP information from the client you will be using as the SAML service provider.
3. Download the IdP metadata.
   This can be used to set up the SAML IdP configuration in your SAML SP client (if allowed by your client).
4. Under *SAML Attribute* click *Create New*, and enter a *SAML Attribute* name that your SAML SP is expecting to identify the user. Select a *User Attribute* for this selection. If you're unsure of which attribute to pick, select *SAML Username*.

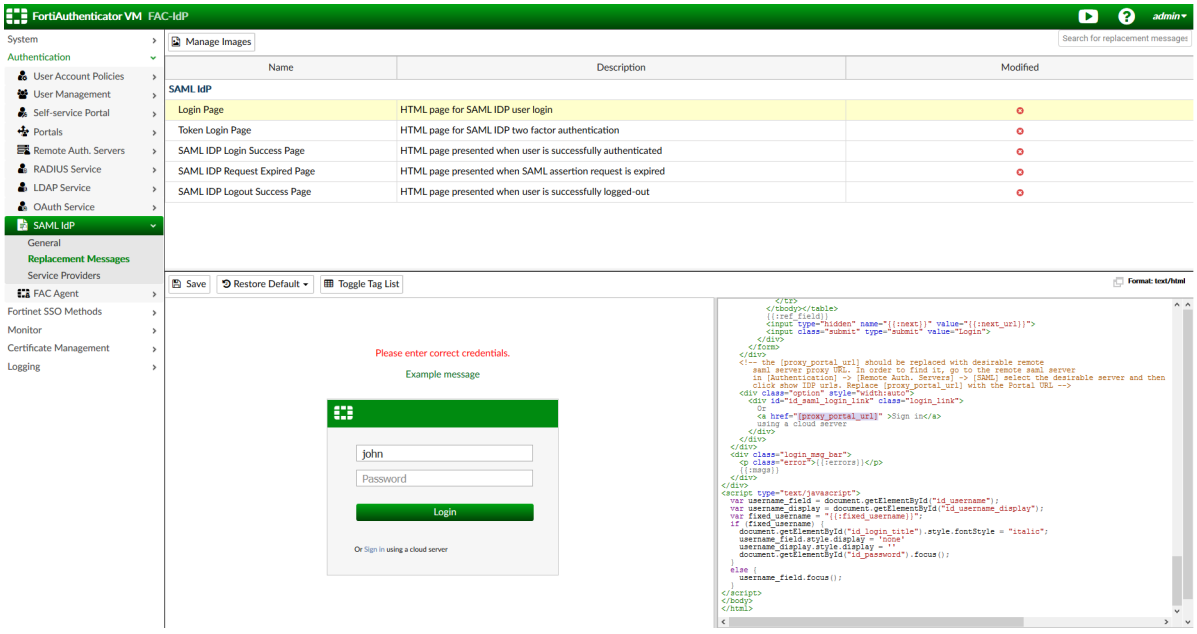


5. Click *OK* to save your changes.

Configuring the login page replacement message

To configure the login page replacement message:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*.
2. On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
3. In the text/html editor, scroll down until you see the `[proxy_portal_url]` placeholder and replace it with the previously saved proxy portal URL.



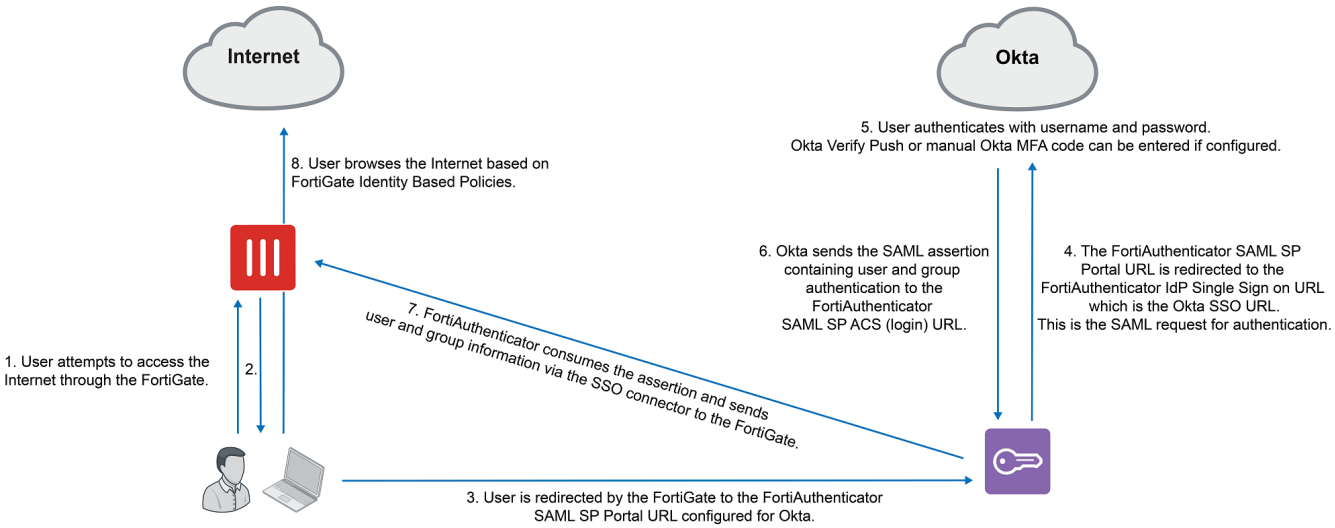
4. Click *Save*.

Results

To test G Suite login through the SP:

1. Enter in the portal login URL from the service provider in a new browser.
   You are redirect you to the FAC's IdP-server and proxy page.
2. Click on the link below the login options to be redirected to Google's login page.

SAML FSSO with FortiAuthenticator and Okta



In this example, you will provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator as the service provider (SP) and Okta, a cloud-based user directory, as the identity provider (IdP).

Okta is a secure authentication and identity-access management service that offer secure SSO solutions. Okta can be implemented with a variety of technologies and services including Office 365, G Suite, Dropbox, AWS, and more.

A user will start by attempting to make an unauthenticated web request. The FortiGate's captive portal will offload the authentication request to the FortiAuthenticator's SAML SP portal, which in turn redirects that client/browser to the SAML IdP login page. Assuming the user successfully logs into the portal, a positive SAML assertion will be sent back to the FortiAuthenticator, converting the user's credentials into those of an FSSO user.

In this example configuration, the FortiGate has a DMZ IP address of `192.168.50.1`, and the FortiAuthenticator has the Port1 IP address of `192.168.50.100`. Note that, for testing purposes, the FortiAuthenticator's IP and FQDN have been added to the host's file of trusted host names; this is not necessary for a typical network.

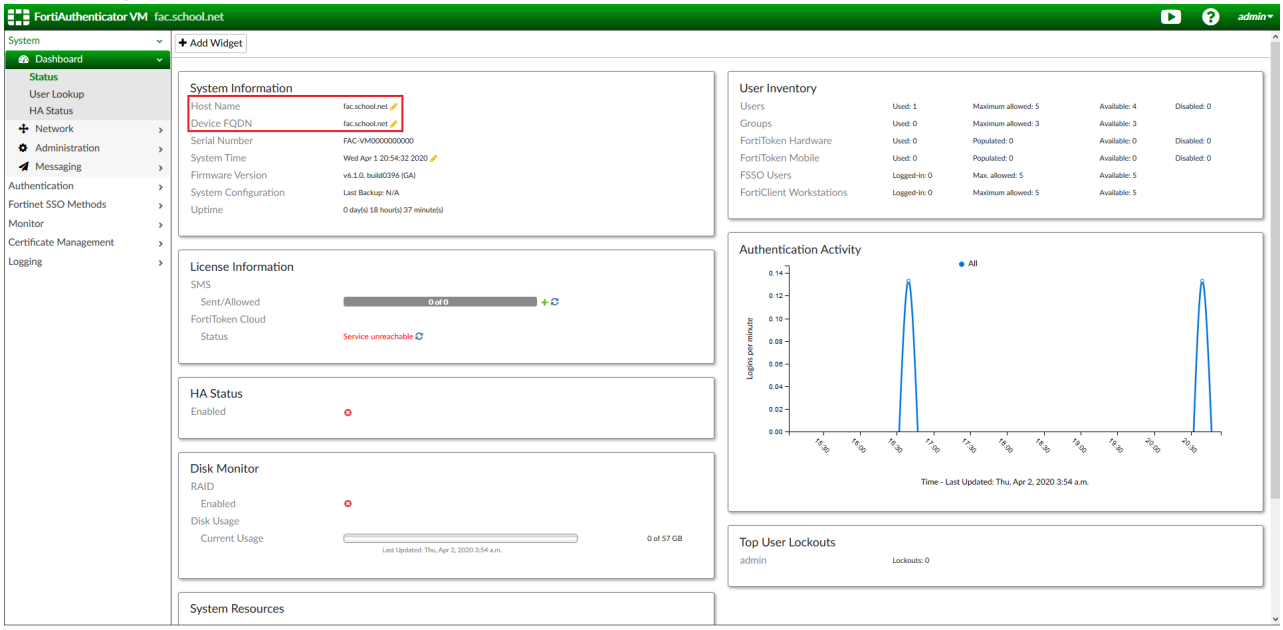
This configuration assumes that you have already created an Okta developer account.

Configuring DNS and FortiAuthenticator's FQDN

1. On FortiAuthenticator, go to *System* > *Dashboard* > *Status*. In the *System Information* widget, select the edit icon next to *Device FQDN*.
   Enter a domain name (in this example, `fac.school.net`). This will help identify where the FortiAuthenticator is

located in the DNS hierarchy.

2. Enter the same name for the *Host Name*. This is so you can add the unit to the FortiGate's DNS list so that the local DNS lookup of this FQDN can be resolved.

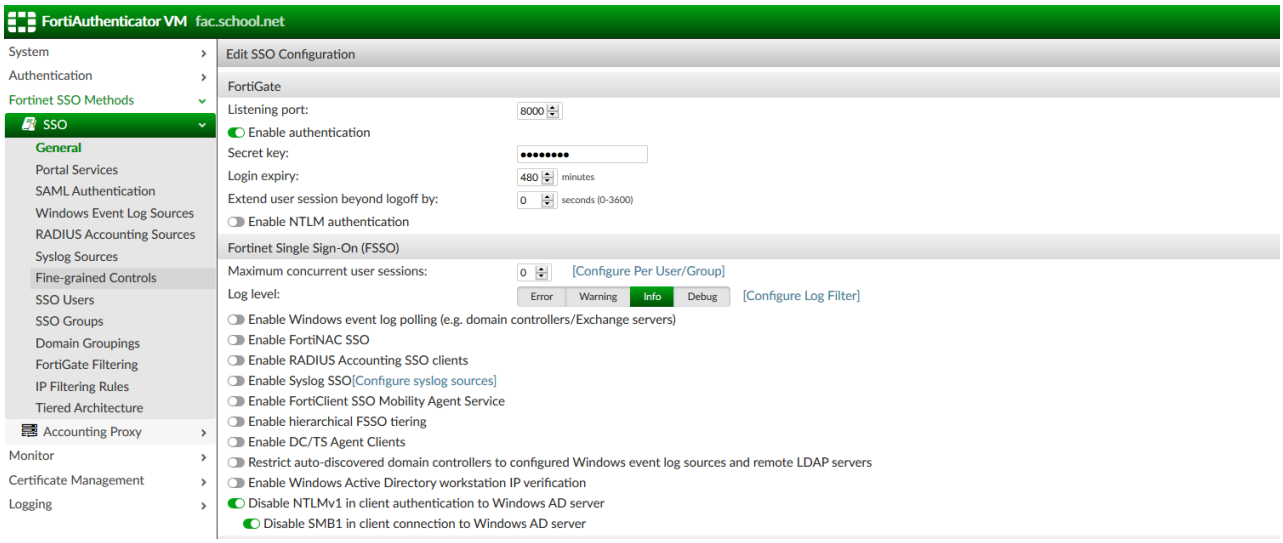


3. On FortiGate, open the CLI Console and enter the following command using the FortiAuthenticator host name and internet-facing IP address.

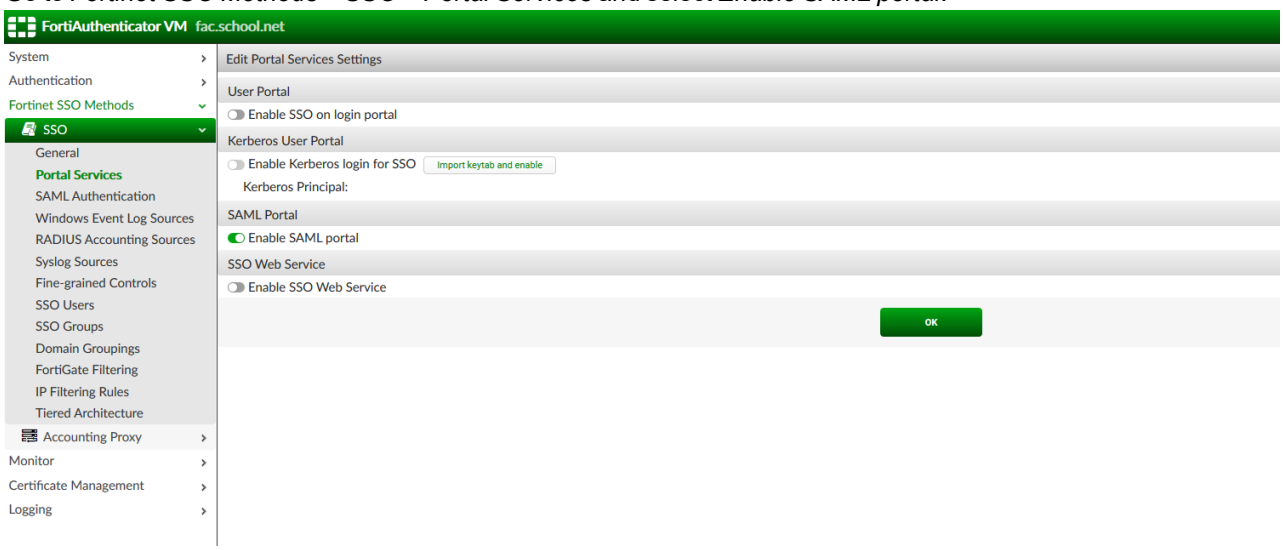
```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 192.168.50.100
         next
      end
      set domain school.net
   next
```

Enabling FSSO and SAML on FortiAuthenticator

1. On FortiAuthenticator, go to *Fortinet SSO Methods* > *SSO* > *General* and set FortiGate SSO options. Make sure to *Enable authentication*.
   Enter a *Secret key* and select *OK* to apply your changes. This key will be used on FortiGate to add the FortiAuthenticator as the FSSO server.

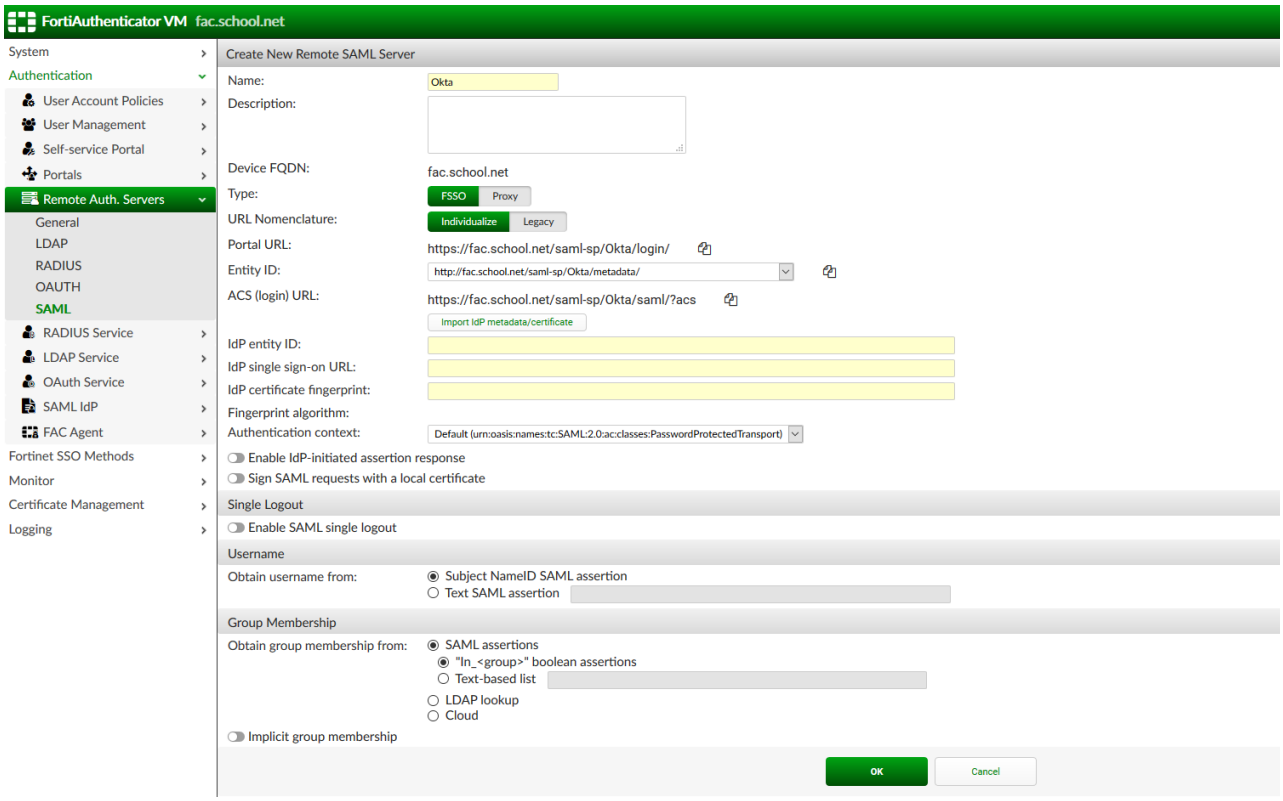


2. Go to *Fortinet SSO Methods* > *SSO* > *Portal Services* and select *Enable SAML portal*.



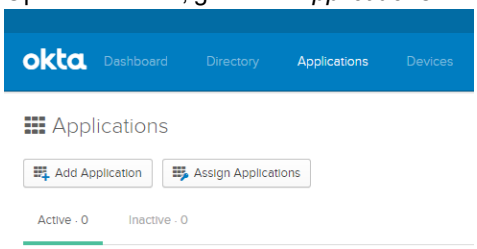
3. Next, go to *Authentication* > *Remote Auth. Servers* > *SAML*, and click *Create New*. Enter Okta as the name.

You will not yet be able to save these settings, as the IdP information - *IdP entity ID*, *IdP single sign-on URL*, and *IdP certificate fingerprint* - must be entered. These fields will be filled out later once the IdP application configuration is complete Okta.

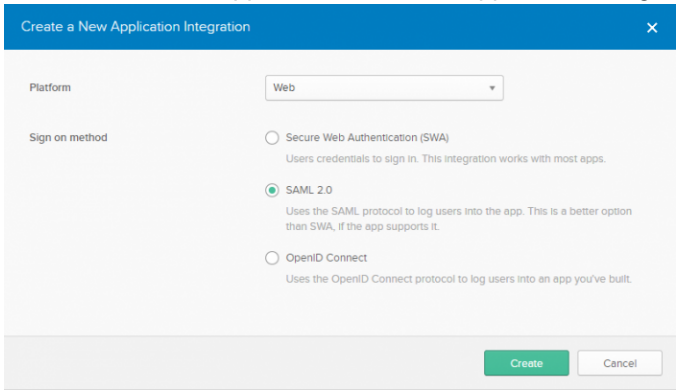


Configuring the Okta developer account IdP application

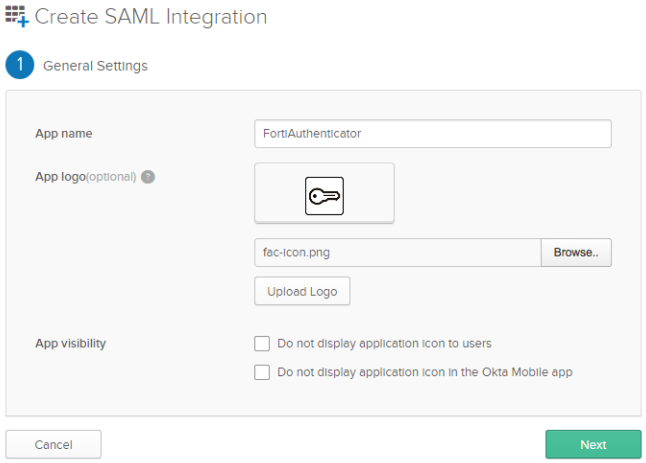
1. Open a browser, go to the *Applications* tab and select *Add Application*.



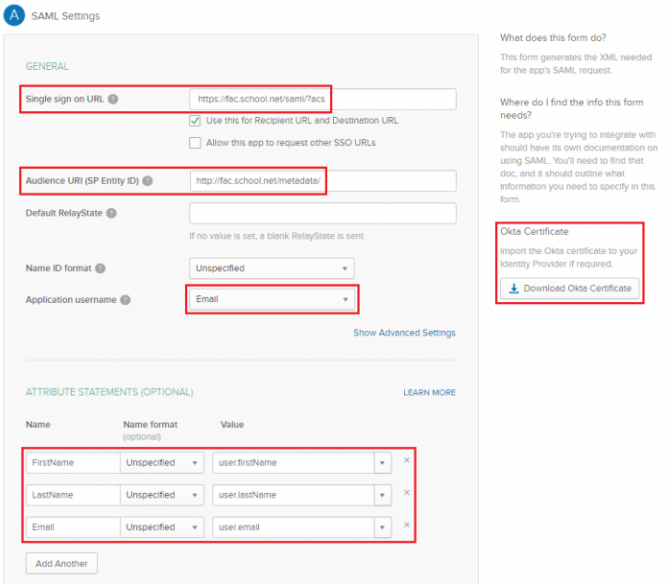
2. Select *Create New App* and create a new application using the SAML 2.0 sign on method.



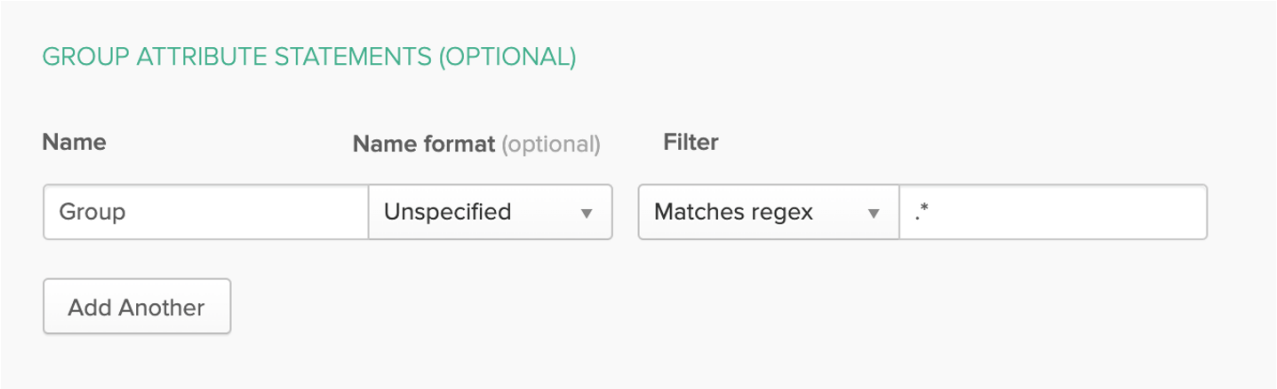
3. Enter a custom app name, and select *Next*. You may upload an app logo if you wish.
The name entered here is the name of the portal that users will log into.



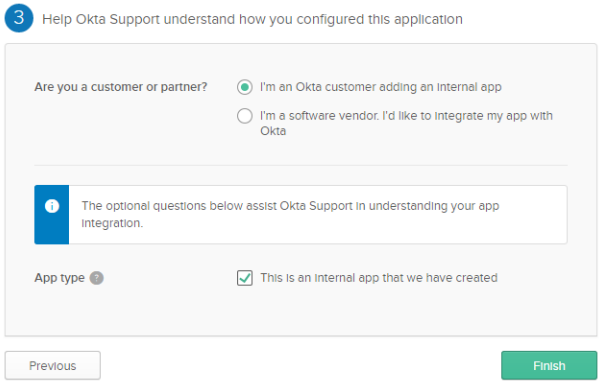
4. Under *A - SAML Settings*, set *Single sign on URL* and *Audience URL (SP Entity ID)* to the *ACS* and *Entity URLs* (respectively) from FortiAuthenticator.
Users will be required to provide their email address as their username, and their first and last names (as seen in the example).
Before continuing, select *Download Okta Certificate*. This will be imported to the FortiAuthenticator later.



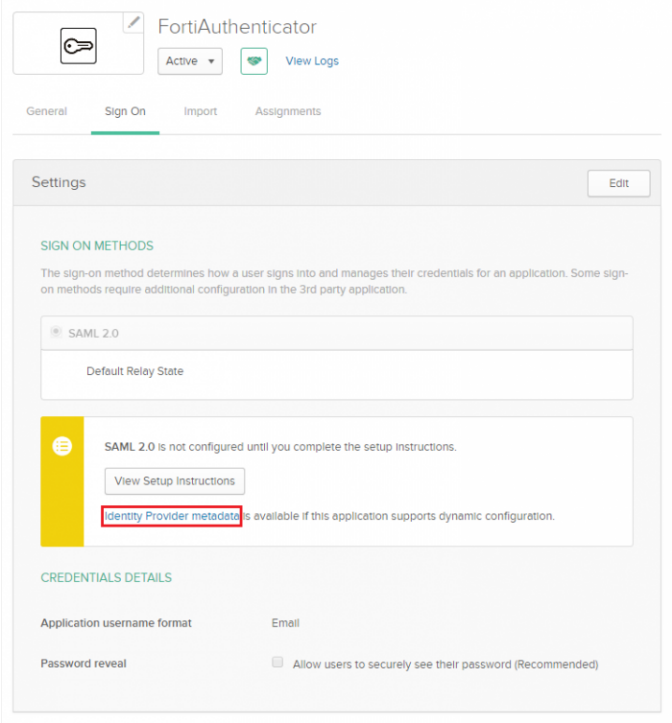
In the section below, configure a *Group* attribute to match on FortiAuthenticator. The word *Group* (case-sensitive) must be entered in *Text-based list* under *Obtain Group Membership from: SAML assertions* inside the remote SAML setup configuration on FortiAuthenticator. Regex matching is the most flexible option for group matching. The below example matches all groups of a single user.



5. In the last step, confirm that you are an Okta customer, and set the *App type* to an internal app. Select *Finish*.

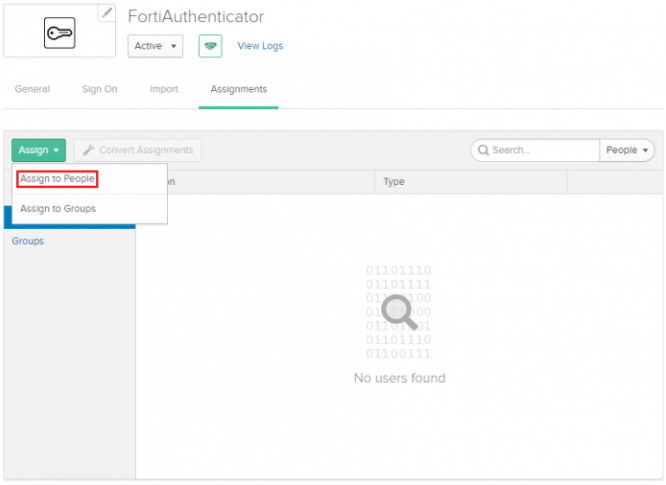


6. Once created, open the *Sign On* tab and download the *Identity Provider metadata*.



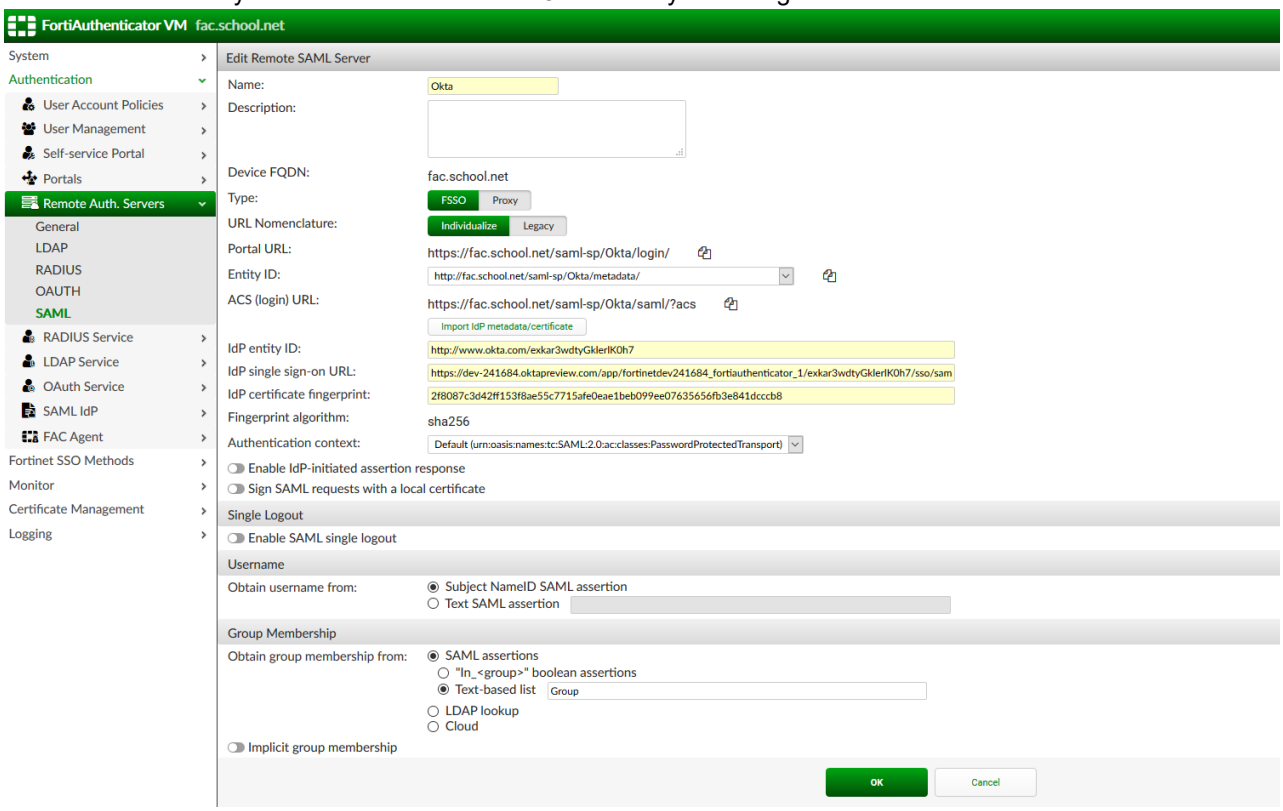
7. Finally, open the *Assignments tab* and select *Assign > Assign to people*.
Assign the users you wish to add to the application. This will permit the user to log in to the application's portal. Save

your changes, and select *Done*.

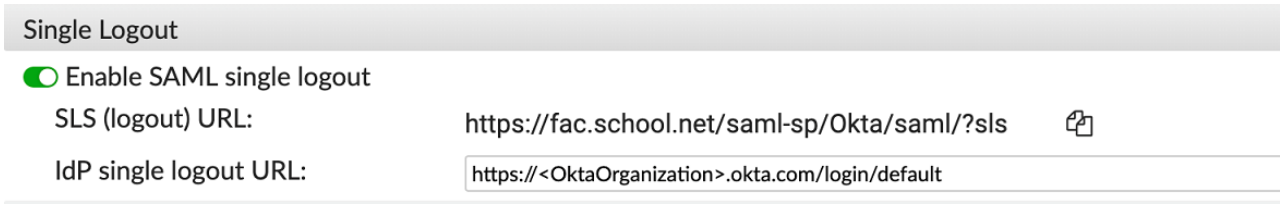


Importing the IdP certificate and metadata on FortiAuthenticator

1. On FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *SAML*, and import the IdP metadata and certificate downloaded from Okta.
   This will automatically fill in the IdP fields. Select *OK* to save your changes.

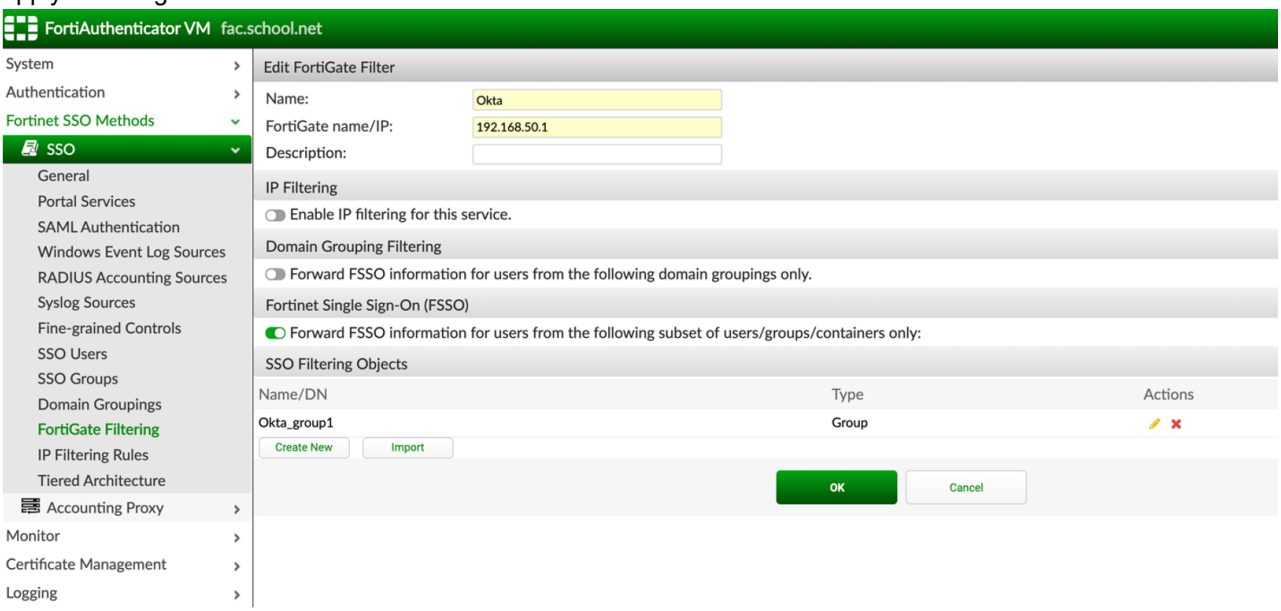


2. Enable SAML single logout and add the *IdP single logout URL* under the *Single Logout* section of the Okta Remote SAML Server.
   For example, if your Okta organization is "facschool" then the *IdP single logout URL*: entry would be `https://facschool.okta.com/login/default`.



3. Go to *Fortinet SSO Methods* > *SSO* > *FortiGate Filtering*, and create a new FortiGate filter.
   Enter a name and the FortiGate's DMZ-interface IP address, and click *OK*.
   Once created, enable *Forward FSSO information for users from the following subset of users/groups/containers only*. Select *Create New* to create SSO group filtering objects that match each group inside Okta, and select *OK* to

apply all changes.

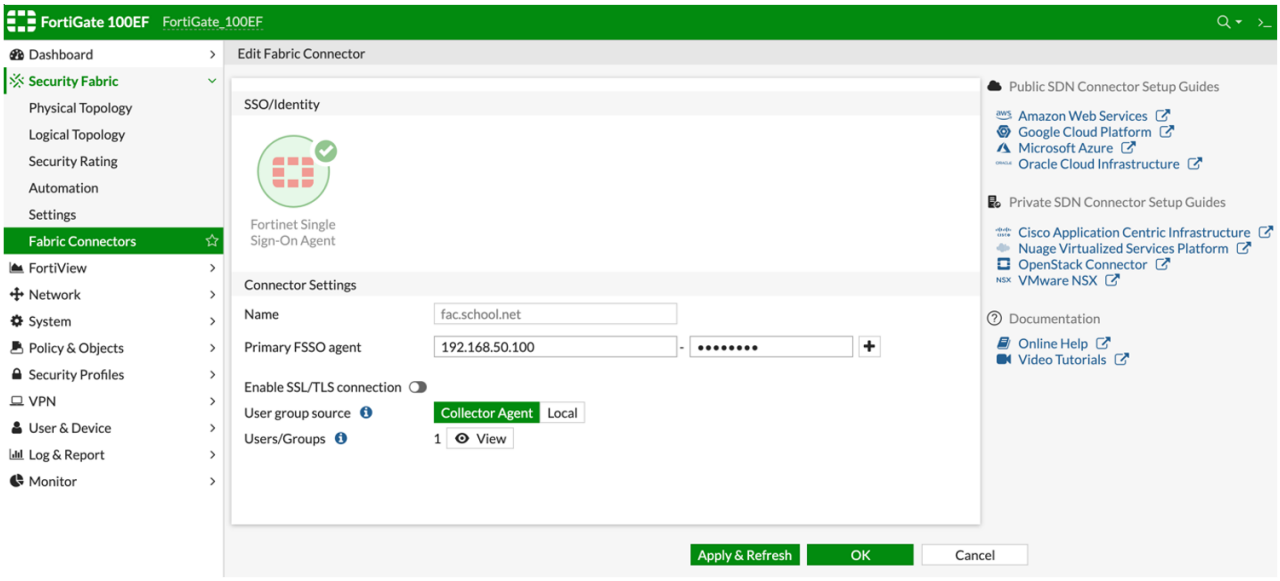


The names entered for the filter must be the same as the group names created in Okta. Failing to enter the exact same names will result in the SSO information not being pushed to FortiGate.

Configuring FSSO on FortiGate

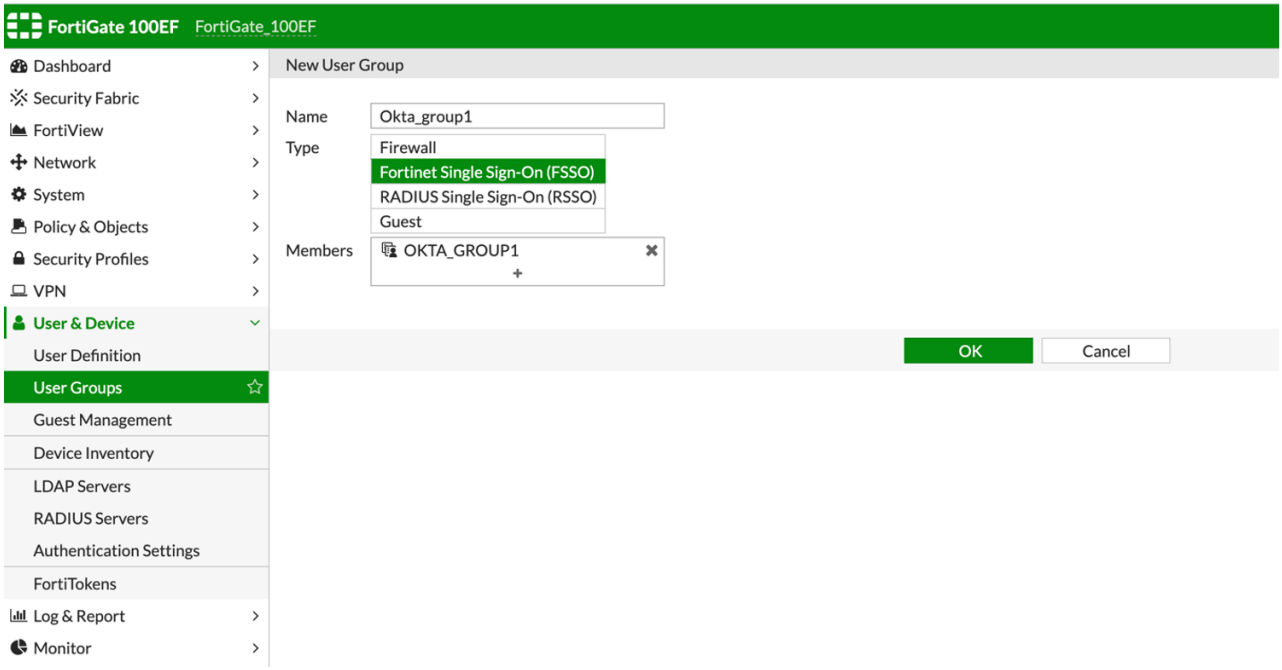
To configure FSSO on FortiGate:

1. On FortiGate, go to *Security Fabric* > *Fabric Connectors*.
   Create a new FSSO agent connector to the FortiAuthenticator.
2. Select *Apply & Refresh*. The SAML user groups name has been successfully pushed to FortiGate from FortiAuthenticator, appearing when you select *View*.



Select *View* and make sure that the FSSO group has been pushed to FortiGate.

3. Go to *User & Device* > *User Groups* and create a new user group.
Enter a name, set *Type* to *Fortinet Single Sign-On (FSSO),* and add the FSSO group as a *Member.*



Configure automatic redirect

To configure automatic redirect on FortiGate:

In order to automatically redirect the user to the initial website after authentication, erase the existing HTML code and replace it with the following HTML code on the FortiGate in *System* > *Replacement Messages* > *Authentication* > *Login Page.*

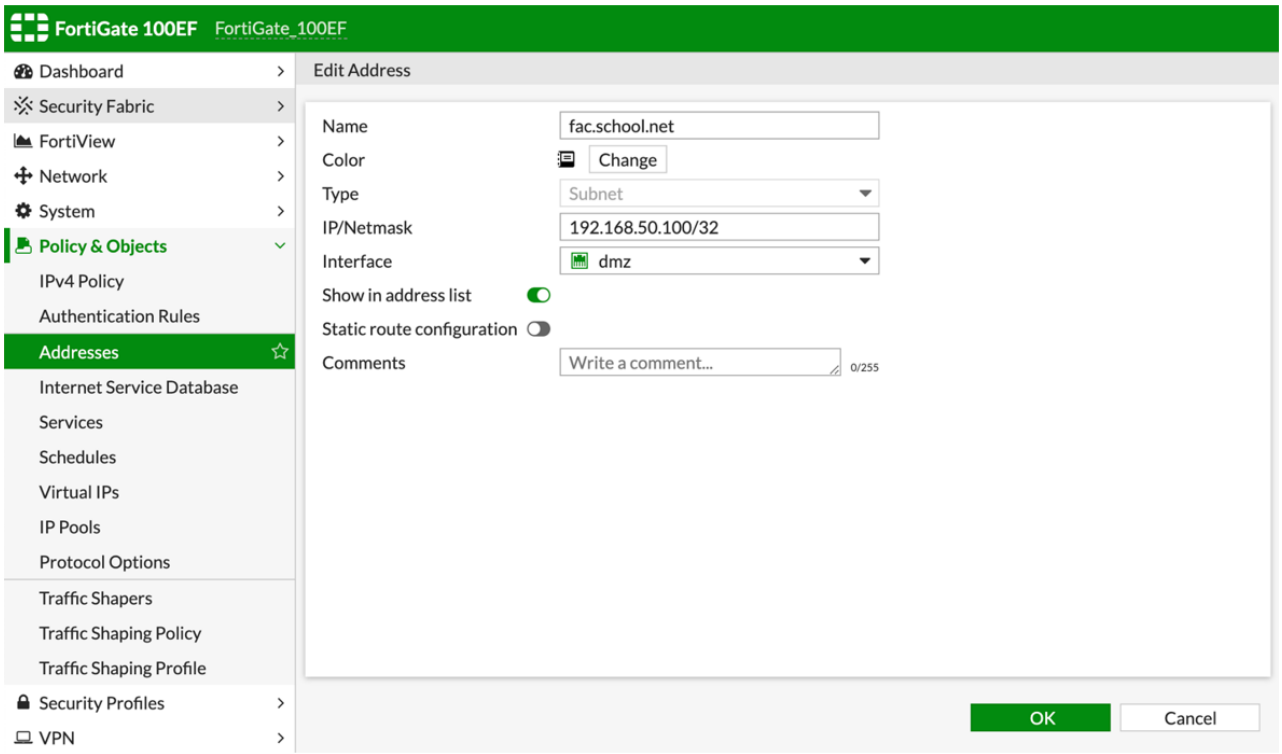
Replace **<FortiAuthenticator-FQDN>** with the DNS name of the FortiAuthenticator.

```
<html>

  <head>

    <meta charset="UTF-8">

    <meta http-equiv="refresh" content="1;url=https://<FortiAuthenticator-FQDN>/saml-sp/Ok-
ta/login/?user_continue_url=%%PROTURI%%&userip=%%USER_IP%%">

    <script type="text/javascript">
      window.location.href="https://<FortiAuthenticator-FQDN>/saml-sp/Okta/login/?user_con-
tinue_url=%%PROTURI%%&userip=%%USER_IP%%"
    </script>

    <title>
      Page Redirection
      <title>

        <head>

          <body>
            If you are not redirected automatically,
            <a href="https://<FortiAuthenticator-FQDN>/saml-sp/Okta/login/?user_continue_url-
l=%%PROTURI%%&userip=%%USER_IP%%">
              login
            </a>

            <body>

              <html>
```

Configure address objects and policies

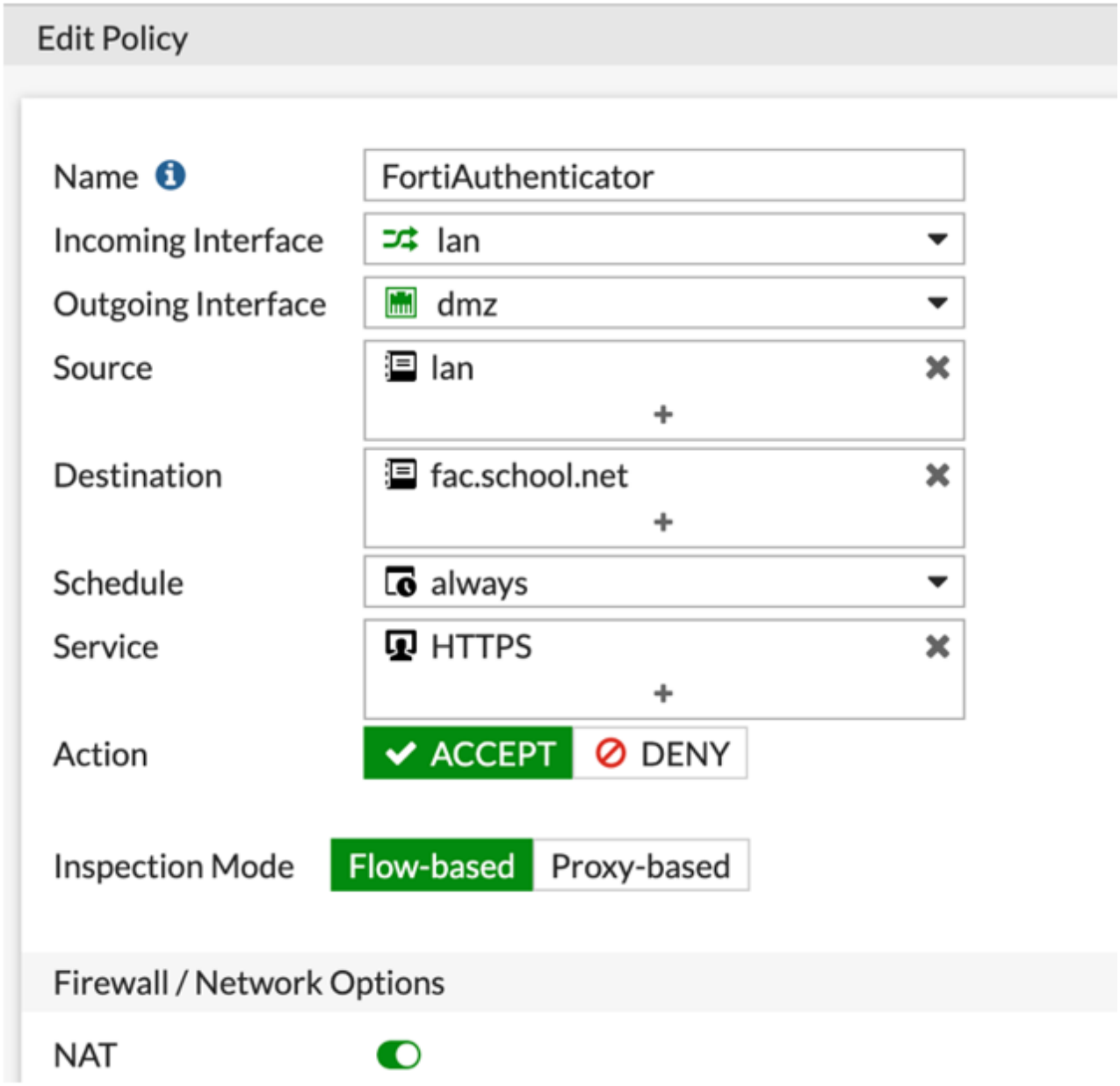
To configure addresses objects and policies on FortiGate:

1. Go to *Policy & Objects* > *Addresses* and add the FortiAuthenticator as an address object.

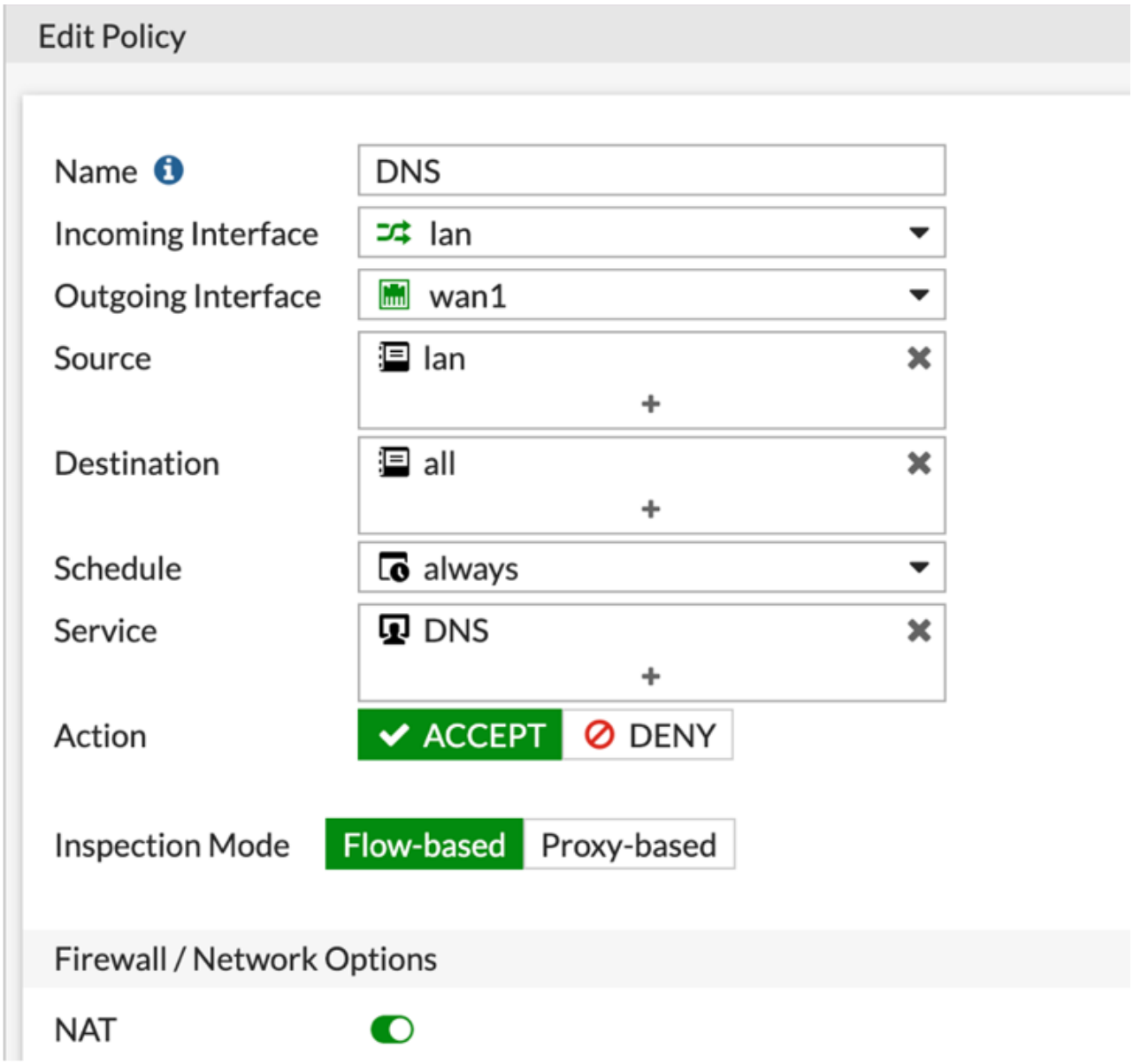


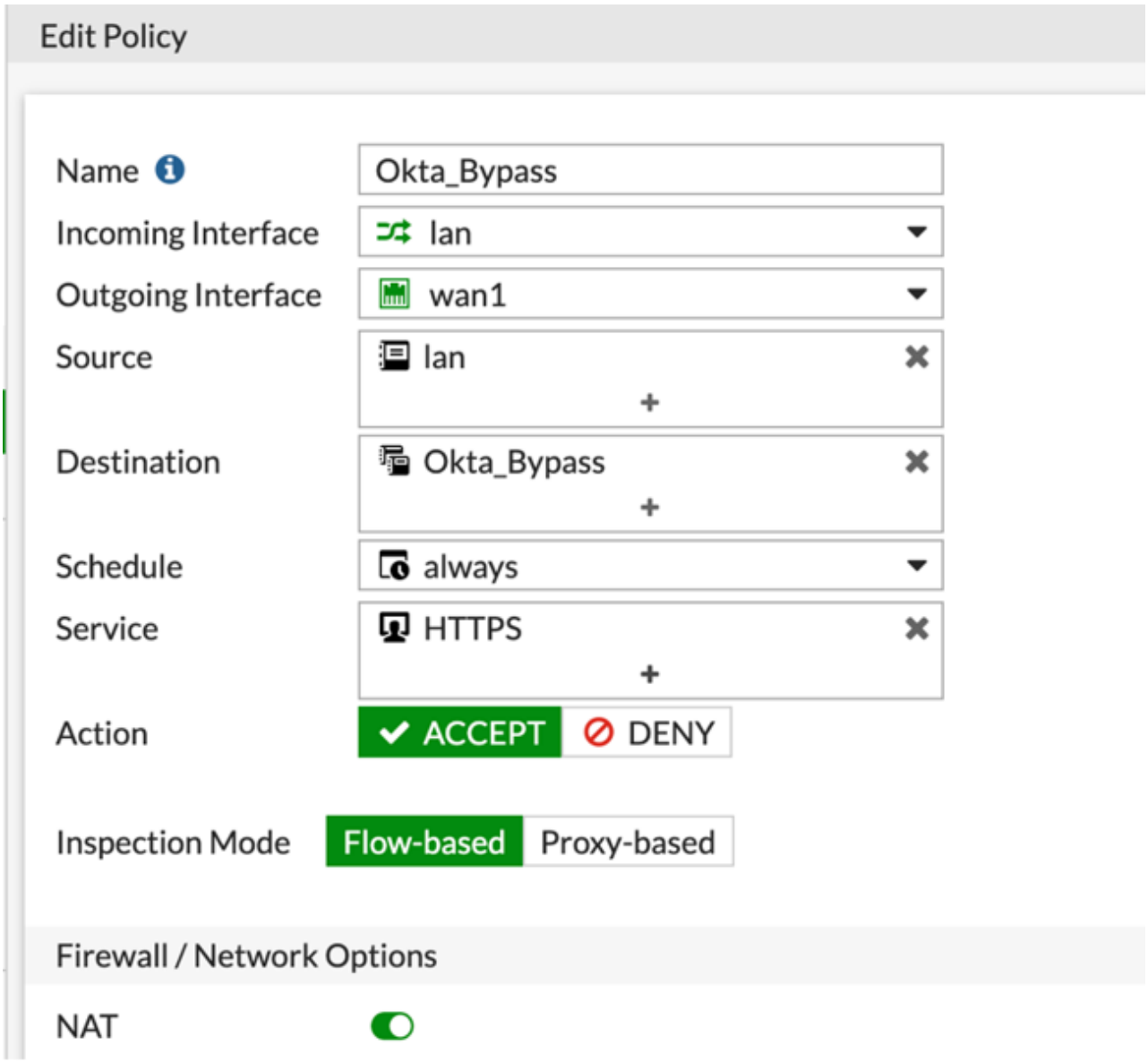
2. Create the FQDN objects below.
   - *.okta.com
   - *.mtls.okta.com
   - *.oktapreview.com
   - *.mtls.oktapreview.com
   - *.oktacdn.com
   - *.okta-emea.com
   - *.mtls.okta-emea.com
   - *.kerberos.okta.com
   - *.kerberos.okta-emea.com
   - *.kerberos.oktapreview.com

   As these are FQDNs, make sure to set *Type* to *FQDN*.
3. Create an *Address group* and name it *Okta Bypass* and add the FQDNs you created above into the Okta Bypass address group.
4. Go to *Policy & Objects* > *IPv4 Policy* and create all policies shown in the examples below: a policy for DNS, for access to the FortiAuthenticator, for Okta bypass, and for FSSO including the SAML user group.
   Allow access to the FortiAuthenticator on the DMZ from the LAN:

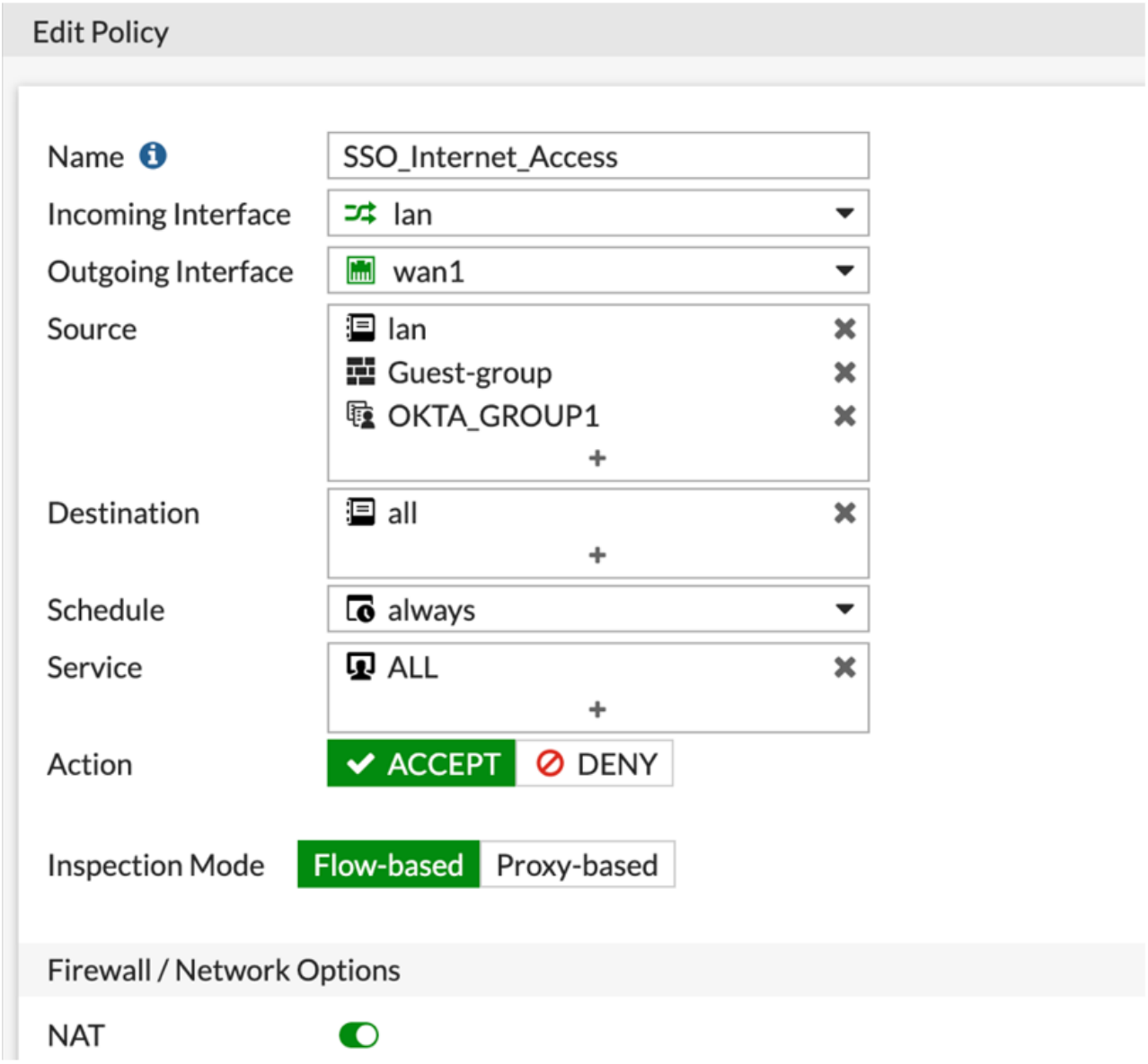


Add the following three policies in order:


Edit Policy
Name
DNS
Incoming Interface
lan
Outgoing Interface
wan1
Source
lan
Destination
all
Schedule
always
Service
DNS
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT



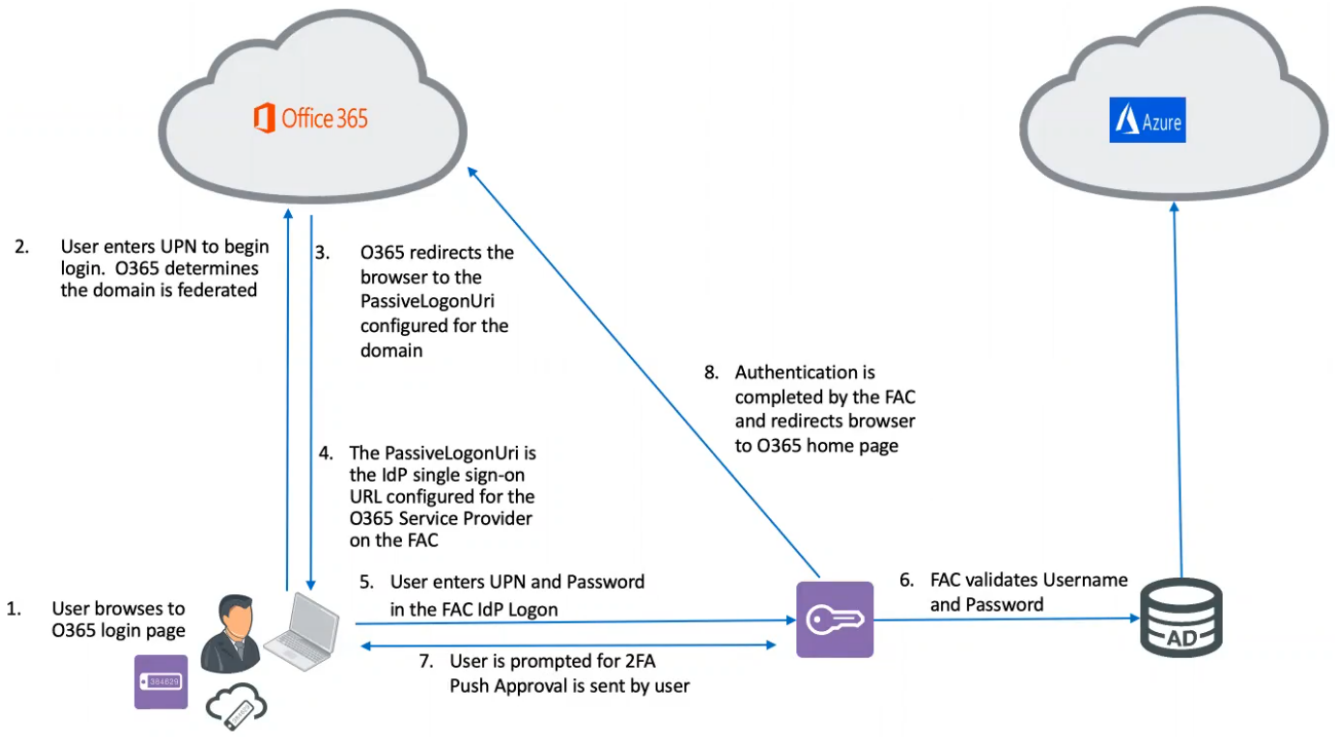
In the *SSO_Internet_Access* policy, add the Firewall *Guest-group* and the Okta FSSO group that is received from FortiAuthenticator. The Guest-group redirects the initial Internet access request from the browser to Okta. Once the user is authenticated the browser will automatically redirect to the website from the initial HTTP/HTTPS request matching the Okta SSO group.



Office 365 SAML authentication using FortiAuthenticator with 2FA

FortiAuthenticator can act as the SAML IdP for an Office 365 SP using FortiToken served directly by FortiAuthenticator or from FortiToken Cloud for two-factor authentication.

The configuration outlined in this guide assumes that you have already configured your FortiAuthenticator with FortiToken Cloud. For more information on how to do this, please see the FortiAuthenticator Administration Guide.



To configure Office 365 SAML authentication using FortiAuthenticator with two-factor authentication:

1. Configure the remote LDAP server on FortiAuthenticator on page 176
2. Configure SAML settings on FortiAuthenticator on page 177
3. Configure two-factor authentication on FortiAuthenticator on page 178
4. Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 179
5. Configure Microsoft Azure AD Connect on page 181

Configure the remote LDAP server on FortiAuthenticator

To configure the LDAP server:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and click *Create New*.
2. Configure the following settings:
   a. **Name**: Provide a name for the remote LDAP server.
   b. **Primary server name/IP**: Enter the IP address for the AD (Active Directory) source.
   c. **Base distinguished name**: Configure the based distinguished name for your AD source.
   d. **Bind type**: Select *Regular*.
   e. **Username/Password**: Enter the username and password for your AD source.
   The remaining settings can be left in their default state.
3. Click *OK* to save your changes.

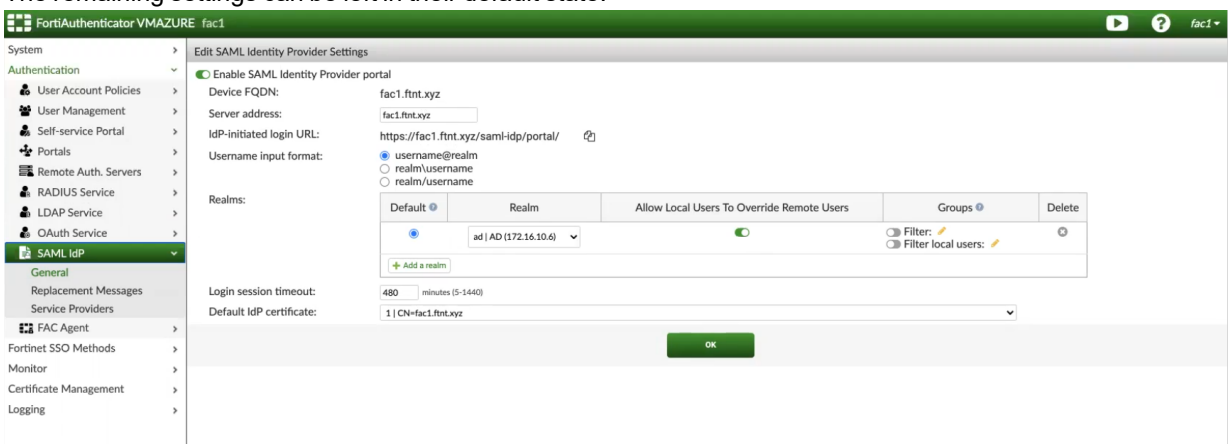
To configure the Active Directory realm:

1. Go to *Authentication* > *User Management* > *Realms* and click *Create New*.
2. Configure a name for the realm and select your LDAP server as the *User source*.
3. Click *OK* to save your changes.

Configure SAML settings on FortiAuthenticator

To configure FortiAuthenticator IdP settings:

1. Go to *Authentication* > *SAML IdP* > *General* and click *Enable SAML Identity Provider portal*.
2. Configure the following settings:
   a. **Server address**: The IP address or FQDN of the FortiAuthenticator.
   b. **Realms**: Select the previously created LDAP realm.
   c. **Default IdP certificate**: Choose a certificate. The default can be used if desired.
   The remaining settings can be left in their default state.

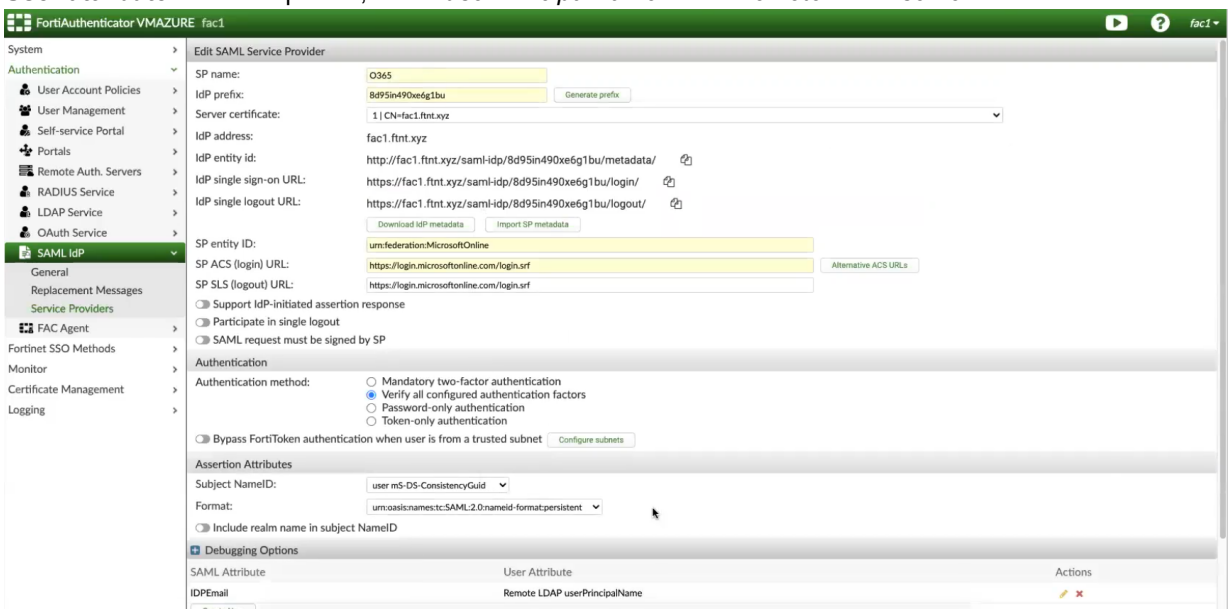


3. Click *OK* to save your changes.

To configure the service provider settings on FortiAuthenticator:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and click *Create New*.
2. Configure the following settings:
   a. **SP Name**: enter a name for your service provider.
   b. **IdP Prefix**: Click *Generate prefix* to create a new IdP prefix.
   c. **Server certificate**: Select the certificate to be used in your configuration or choose *Use default setting in SAML IdP General page*.
   d. **SP entity ID**: Enter `urn:federation:MicrosoftOnline`.
   e. **SP ACS (login) URL**: Enter `https://login.microsoftonline.com/login.srf`.
   f. **SP SLS (logout) URL**: Enter `https://login.microsoftonline.com/login.srf`.
   g. **Participate in single logout**: Can be enabled if you wish this SP to participate in SAML single logout.
3. In the *Assertion Attributes* section, configure the following settings:
   a. **Subject NameID**: Select *user mS-DS-Consistency Guid*.
   b. **Format**: Select *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent*.
   Press `Enter` and then SAML attributes can be created.

4. In the *Debugging Options* section click *Create New* to create a SAML attribute with the following settings:
   a. **SAML attribute**: Enter `IDPEmail`.
   b. **User attribute**: In the dropdown, select *userPrincipalName* under *Remote LDAP server*.

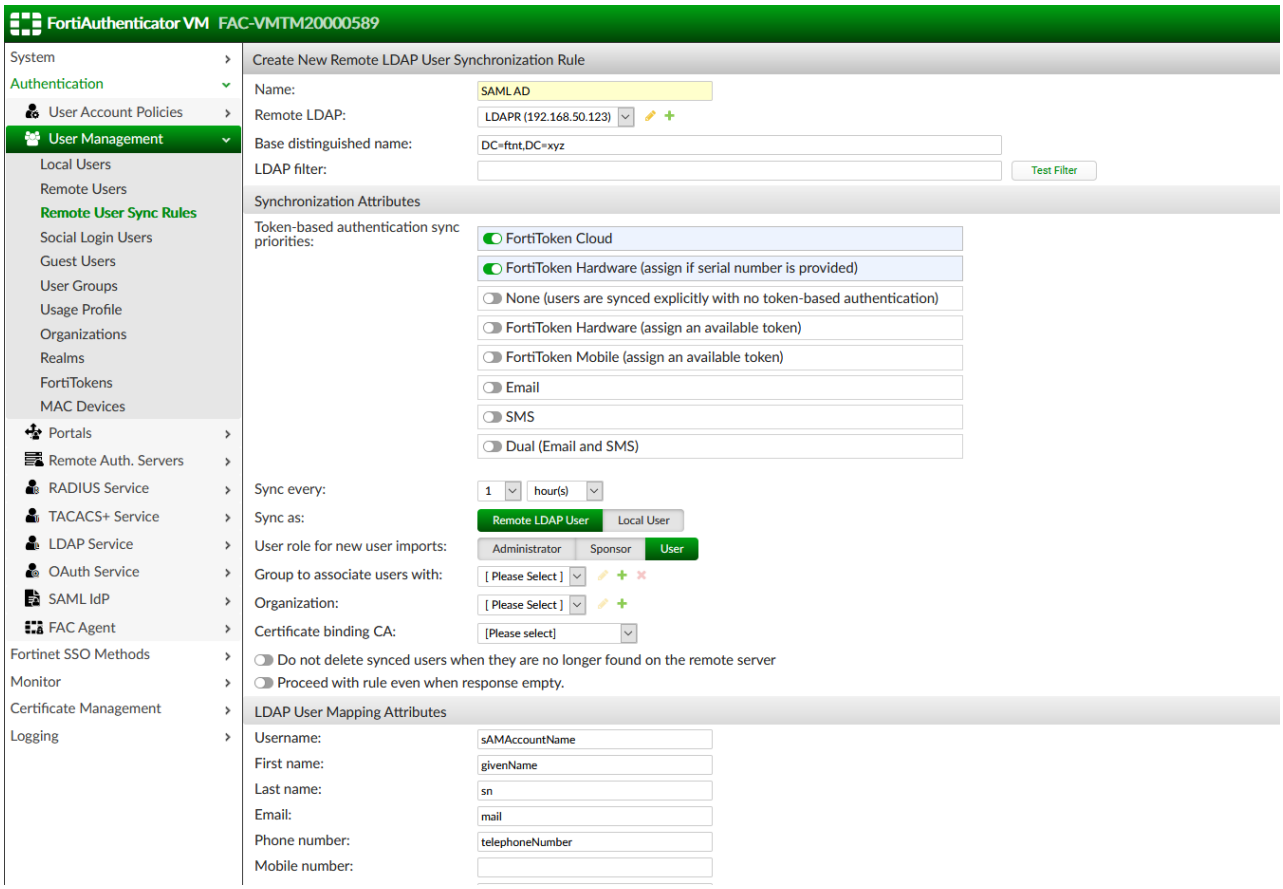


5. Click *OK* to save your changes.

Configure two-factor authentication on FortiAuthenticator

To configure a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*, and click *Create New*.
2. Configure the following settings:
   a. **Name**: Enter a name for the sync rule (e.g. AD).
   b. **Remote LDAP**: Select your remote LDAP server.
3. Configure the token-based sync priority settings under *Synchronization Attributes* by enabling and ordering the authentication sync priorities.
   This example scenario uses FortiToken Cloud for two-factor authentication, so the priority is *FortiToken Cloud* followed by *None (users are synced explicitly with no token-based authentication)*.



4. Select or create a user group to associate users with from the dropdown menu.
5. The remaining settings can be configured to your preference or left in their default state.
6. Click *OK* to save your changes when completed.

To configure remote users with two-factor authentication:

1. Go to *Authentication* > *User Management* > *Remote Users* and *Import* users from your Active Directory account.
2. Edit a user and enable *Token-based authentication*, and select *FortiToken* > *Cloud* as the delivery method.
3. Click *OK* to save your changes.

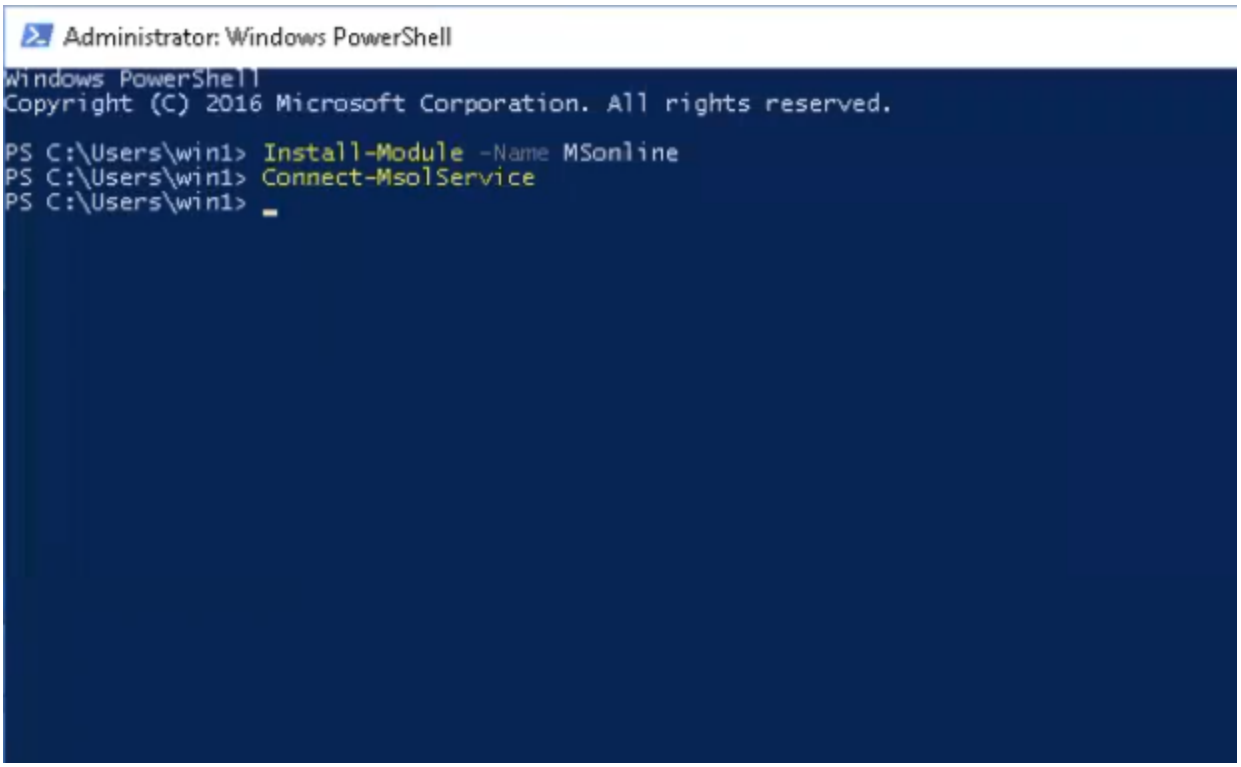
Configure the domain and SAML SP in Microsoft Azure AD PowerShell

FortiAuthenticator currently supports use with Microsoft Azure Active Directory Module for Windows PowerShell.

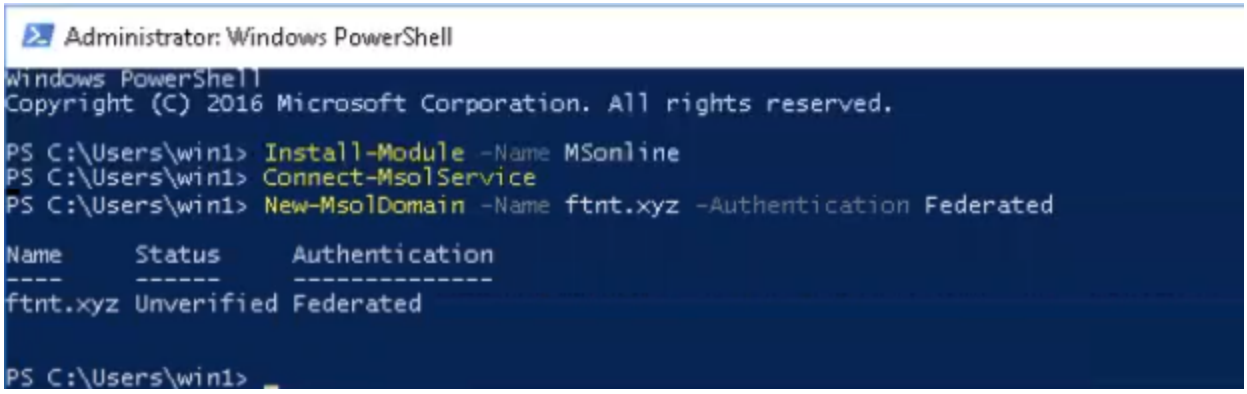
To configure the domain and SAML SP using Microsoft Azure AD PowerShell:

1. Launch the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Enter the following command in PowerShell:
   `Install-Module -Name MSonline.`
   Accept the next two default ("Y") prompts for installing the NuGet Provider and installing from PSGallery.

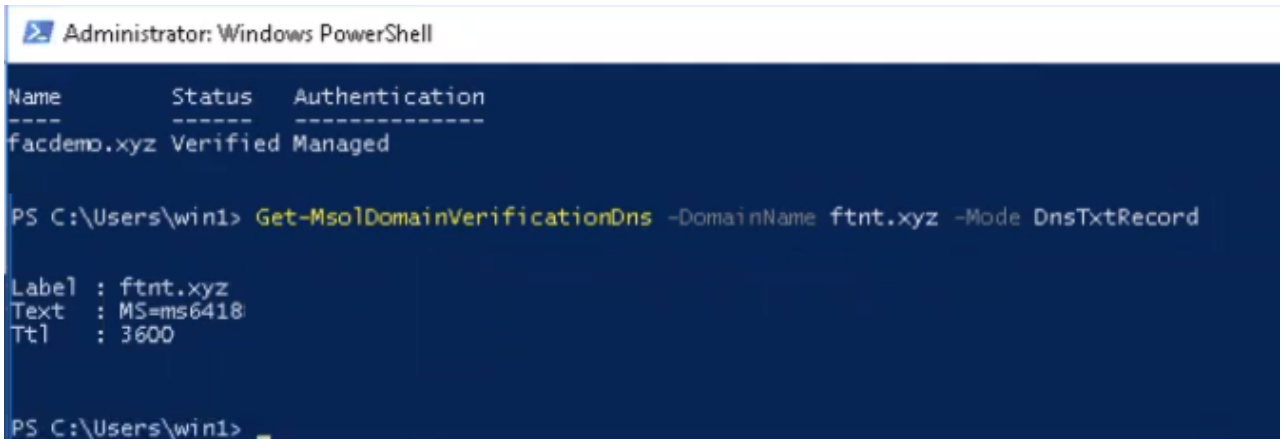
1. If you are using Windows 2016 or earlier, you must first enable TLS 1.2 enforcement for Azure AD Connect. For instructions on enabling TLS 1.2 eforcement, see Azure AD Connect: TLS 1.2 enforcement for Azure Active Directory Connect.

3. Enter the following command:
```
Connect-MsolService .
```


The Microsoft Sign in window opens. Login with your Azure ID.

4. Add a federated domain by entering the following command.
```
New-MsolDomain -Name <your domain> -Authentication Federated
```


5. Obtain the DNS record and create a new text record in your domain provider to allow the domain to be verified. To obtain the DNS record, use the following command:
```
Get-MsolDomainVerificationDns -DomainName ftnt.xyz -Mode DnsTxtRecord
```



From the output, copy the *Text* field results and create a new text record in your domain with a 60 minute interval.

6. Configure the domain as a SAML service provider.
You can create these variables inside a text editor and then copy and paste them into a PowerShell window.

```
$domain = "<your domain>"
$cert = "<your certificate. This can be obtained by downloading your certificate
from FortiAuthenticator and opening it with a text editor.>"
$protocol = "SAMLP"
$IssuerUrl = "<The IdP entity ID from FortiAuthenticator>"
$LogonUrl = "<The IdP single sign-on URL from FortiAuthenticator>"
$LogoffUrl = "<The IdP single logout URL from FortiAuthenticator>"
```

Once completed, enter the following command into PowerShell to verify the domain:

```
Confirm-MsolDomain -DomainName $domain - SigningCertificate $cert -
PreferredAuthenticationProtocol $protocol -IssuerUri $IssuerUrl -PassiveLogOnUri
$LogonURL -LogOffUri $LogOffUrl
```

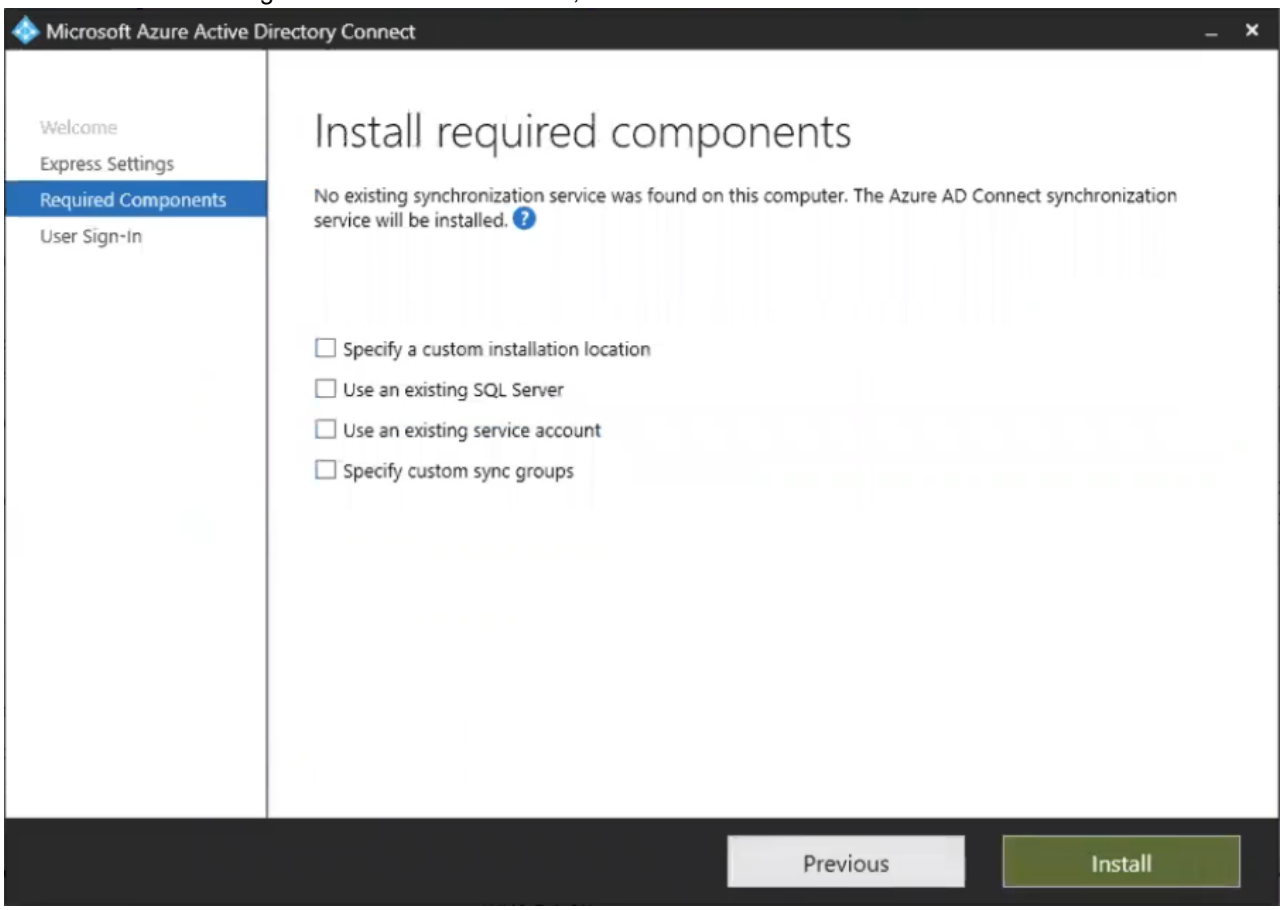
The return text from the above command should read "AvailableImmediately The domain has been successfully verified for your account."

Configure Microsoft Azure AD Connect

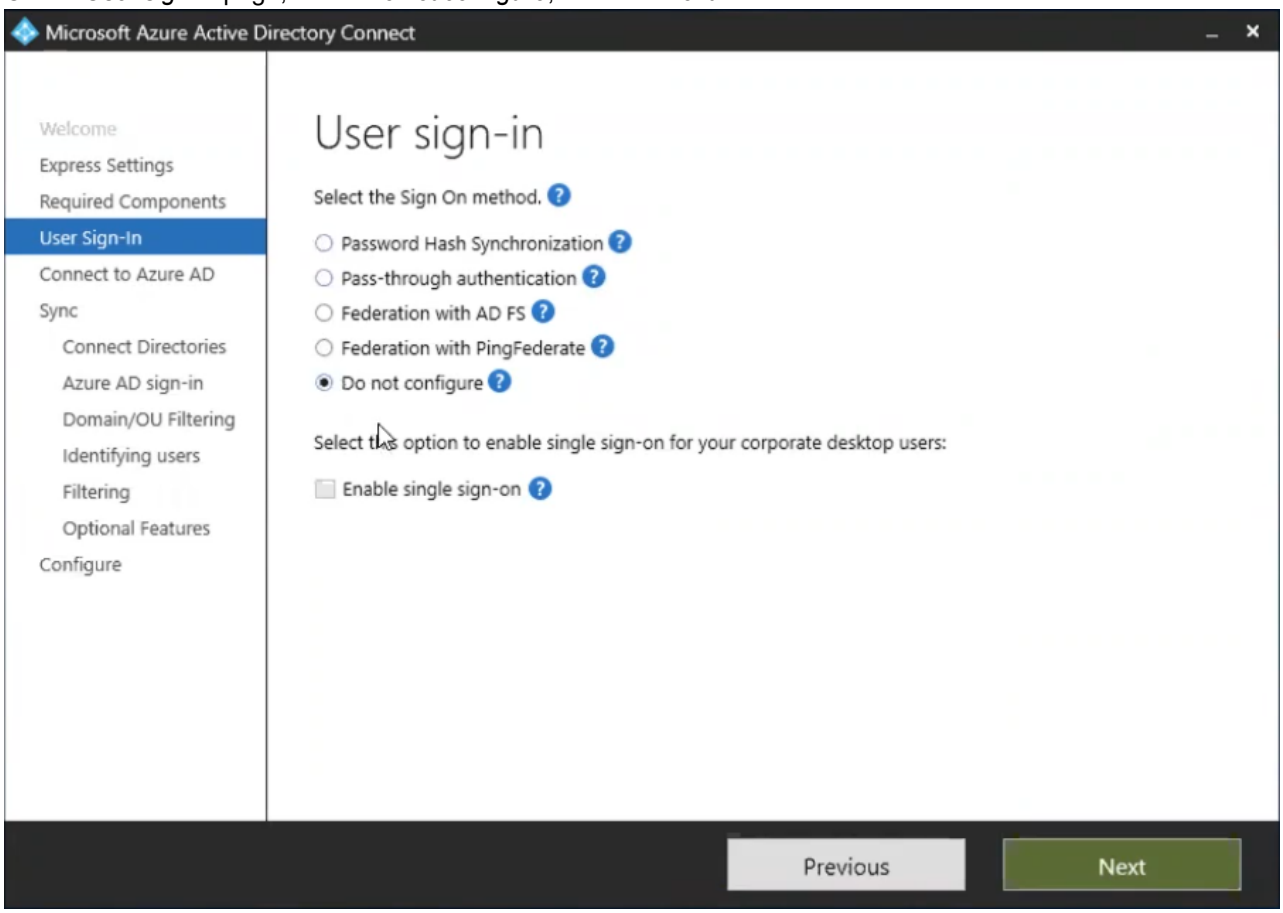
You will first need to download Azure AD Connect from Microsoft on your Active Directory Domain Controller.

To configure Microsoft Azure AD Connect:

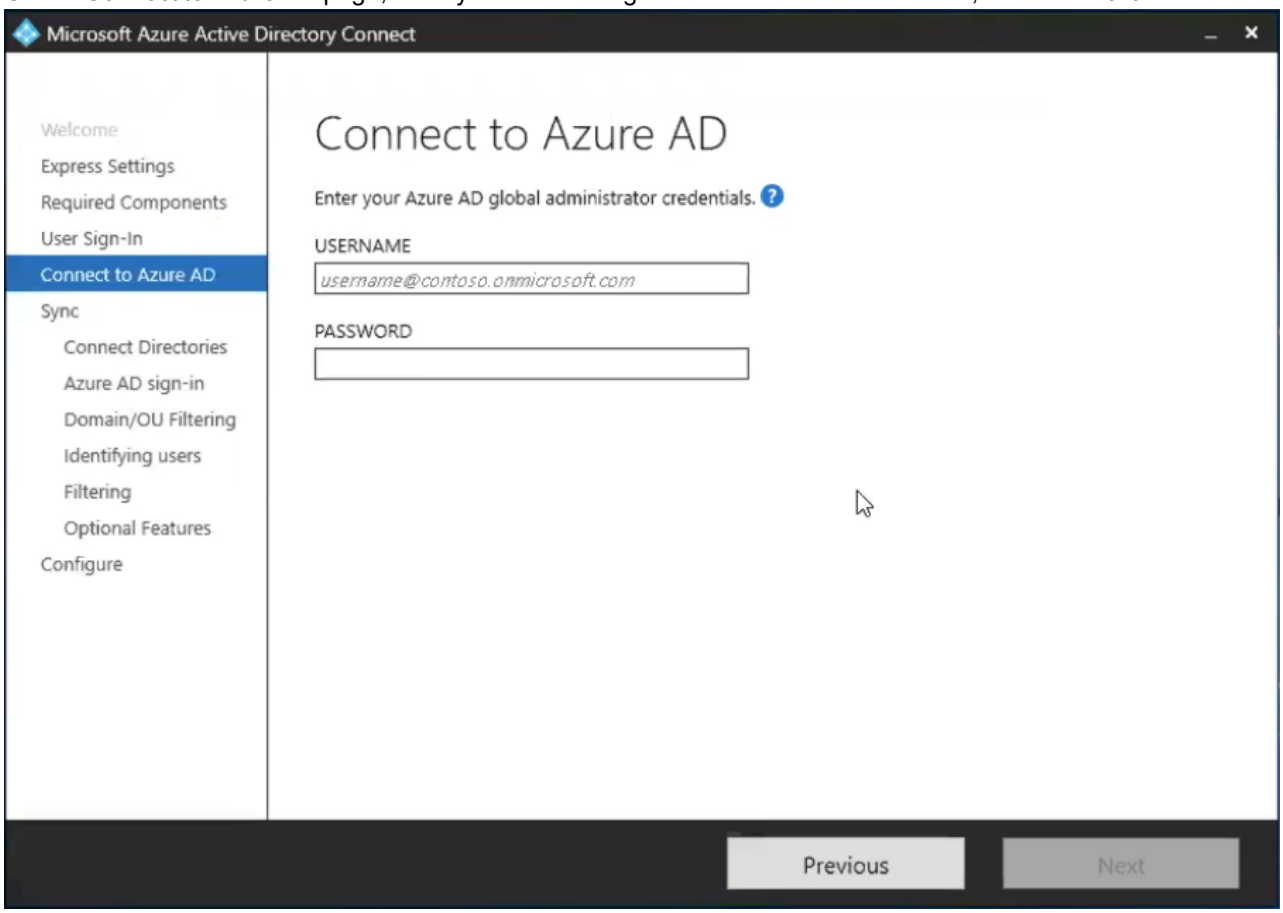
1. Launch Microsoft Azure Active Directory Connect to create a synchronization service to sync attributes from Active Directory to Office365.
2. Select *Customize* to begin a customized installation, and click *Install*.



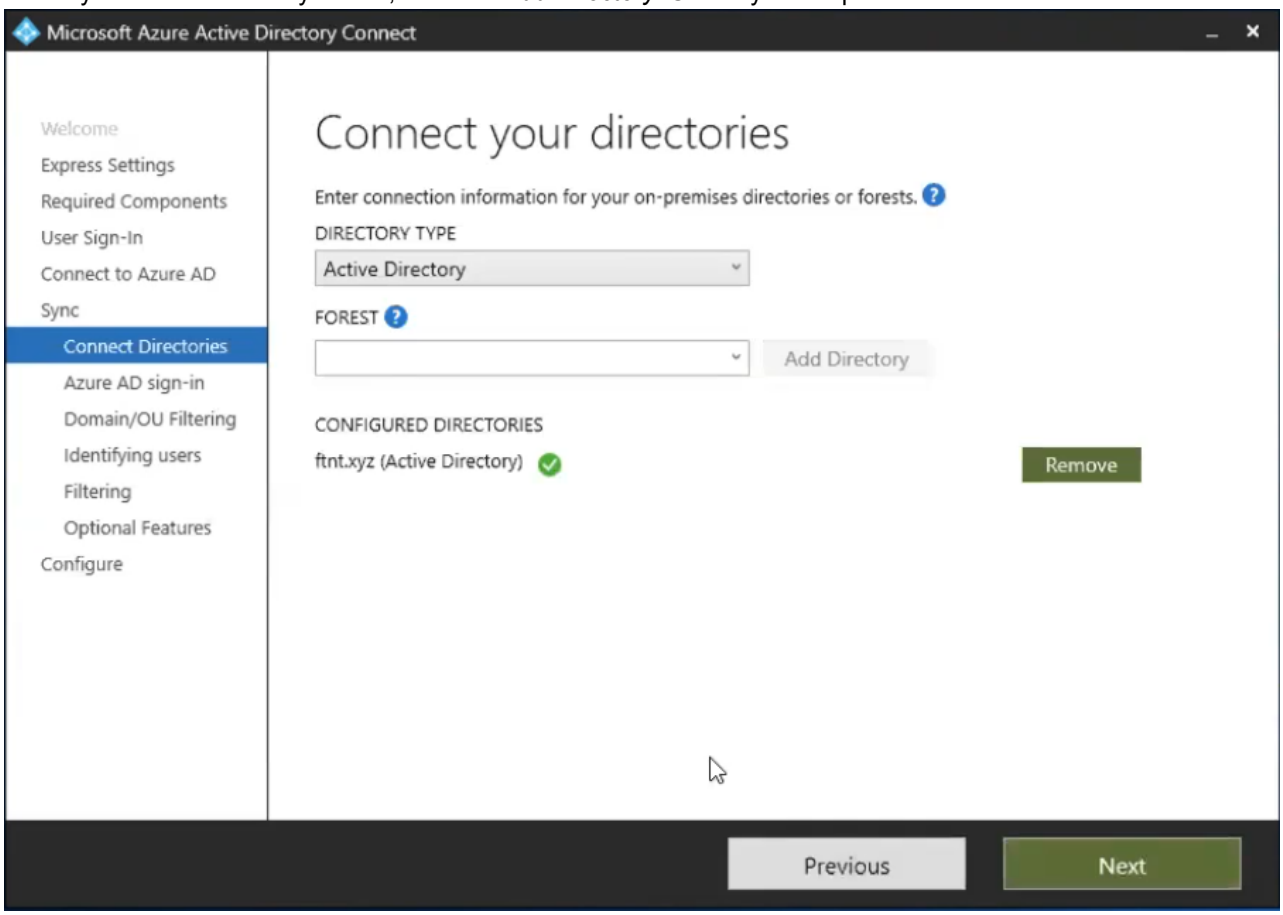
3. On the *User sign-in* page, select *Do not configure*, and click *Next*.



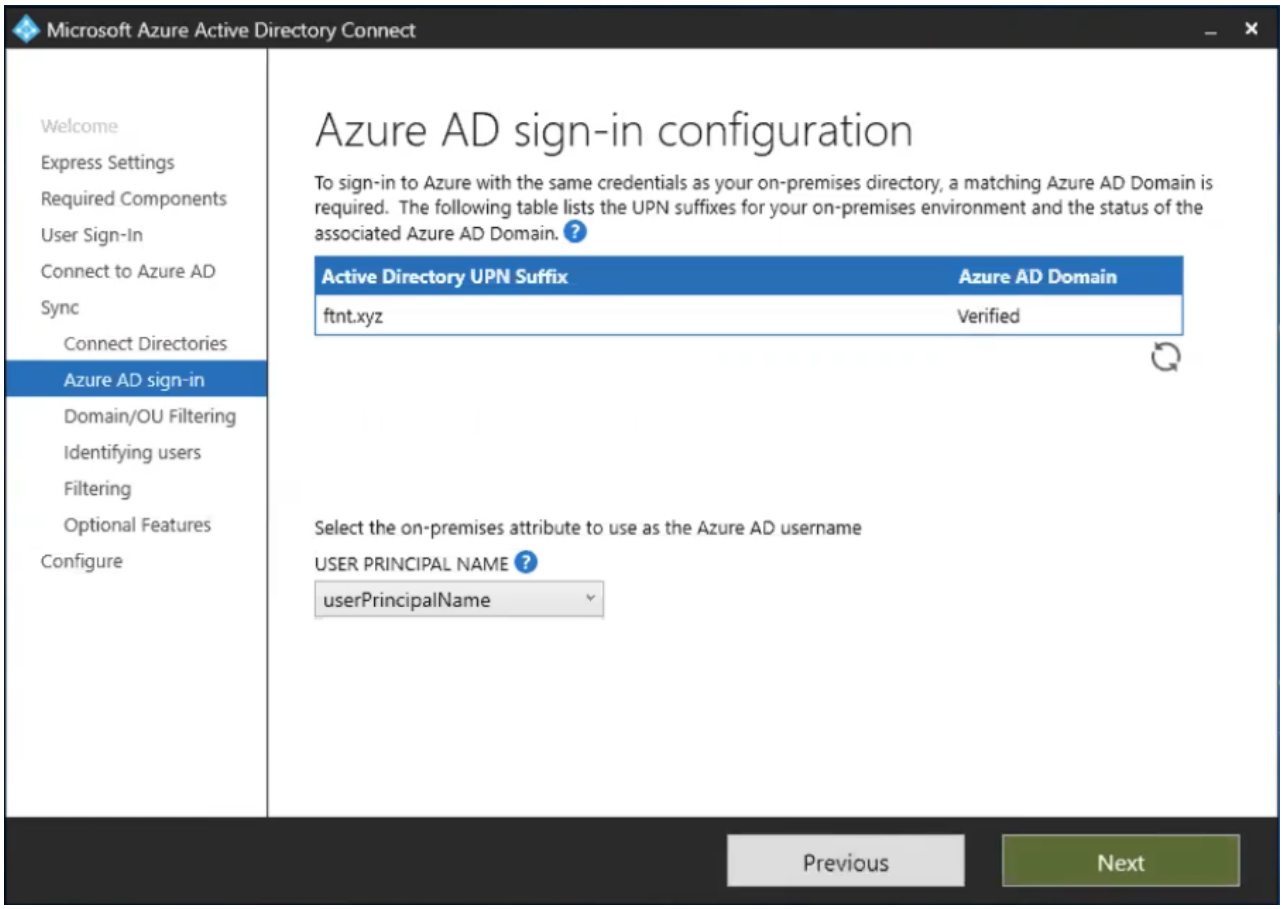
4. On the *Connect to Azure AD* page, enter your Azure AD global administrator credentials, and click *Next*.



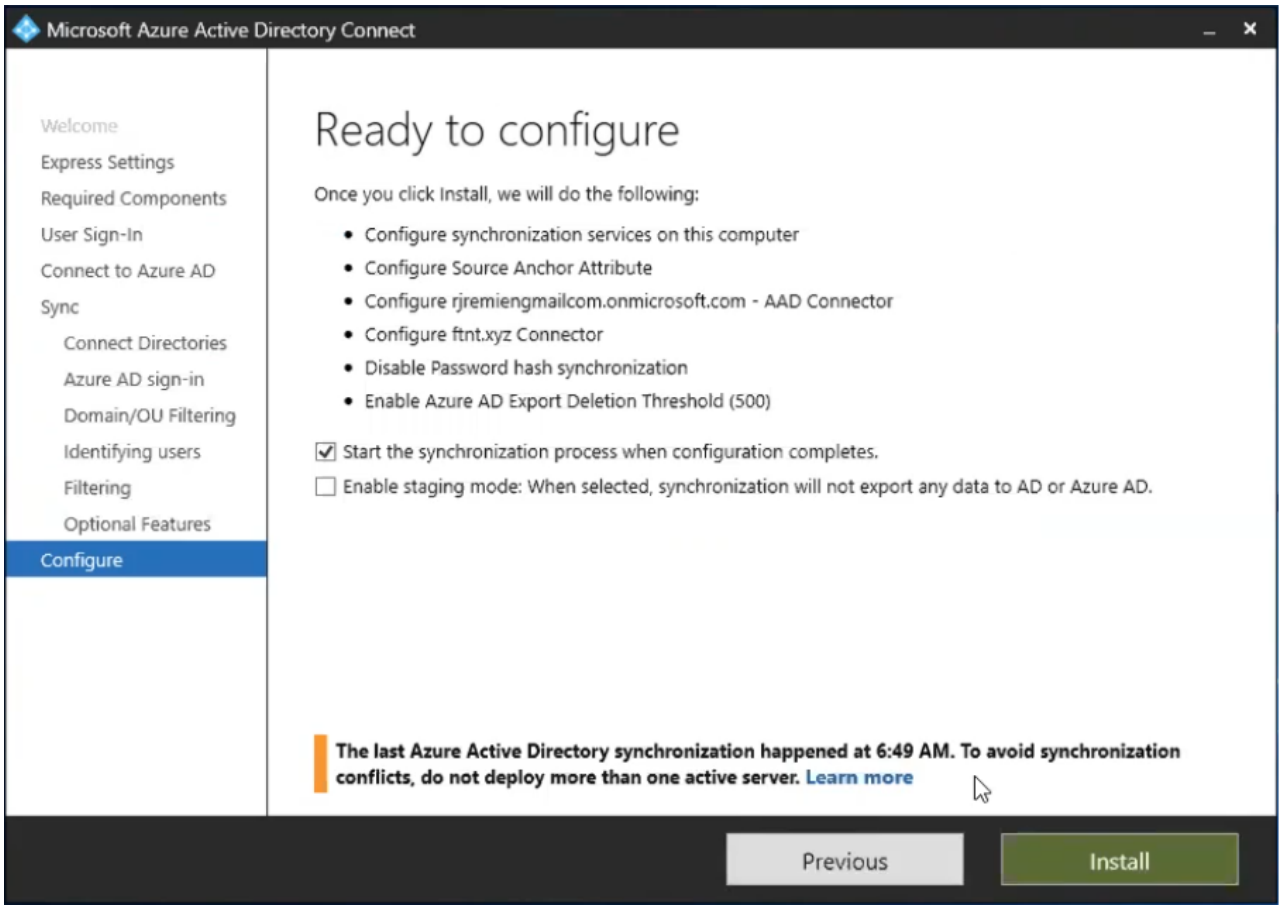
5. Select your Active Directory Forest, and click *Add Directory*. Create your on-premise AD admin user account.



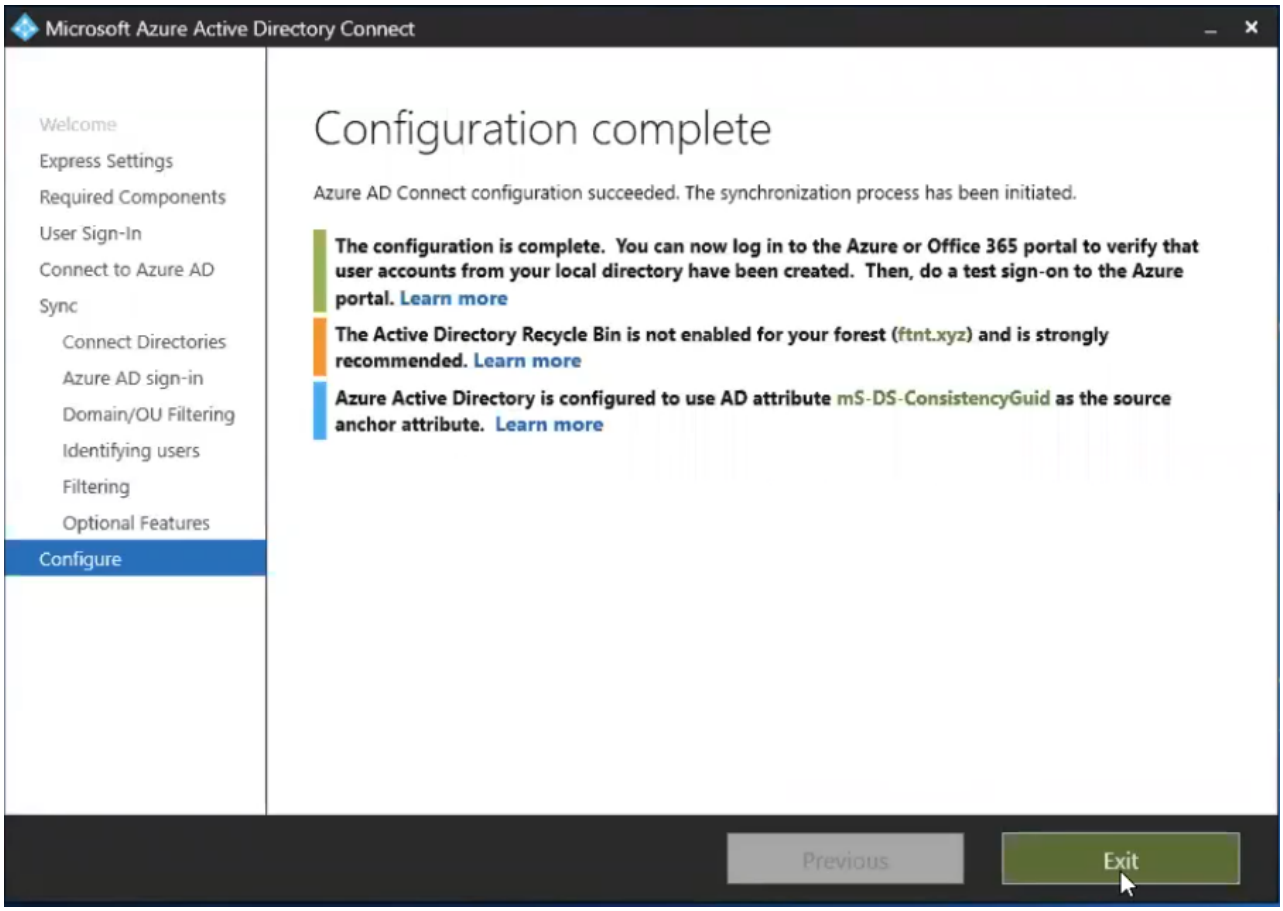
When finished, click *Next*. If completed successfully, you will see your domain has been verified.
Click *Next* again.


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Azure AD sign-in configuration
To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.
Active Directory UPN Suffix
Azure AD Domain
ftnt.xyz
Verified
Select the on-premises attribute to use as the Azure AD username
USER PRINCIPAL NAME
userPrincipalName
Previous
Next

6. Click *Next* on the remaining pages in the configuration wizard, and click *Install* on the *Ready to configure* page.



7. Once the installation is complete, you are presented with the Configuration complete page which provides a summary of the configuration changes.

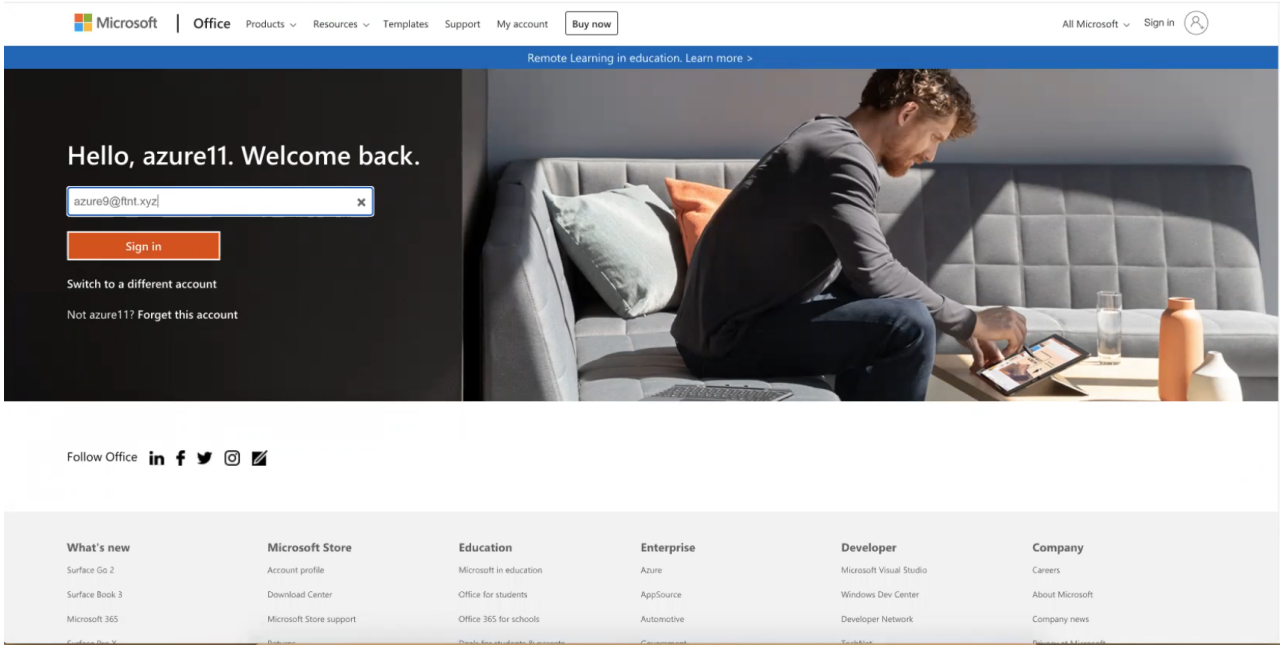


Results

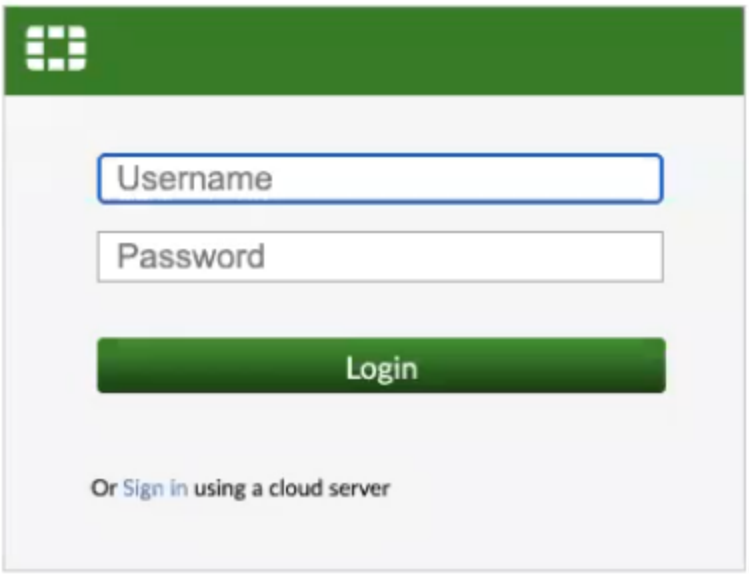
Once configured, Active Directory synchronized users can sign in to Office 365 using two-factor authentication from FortiAuthenticator.

To sign in to Office 365 using FortiAuthenticator with two-factor authentication:

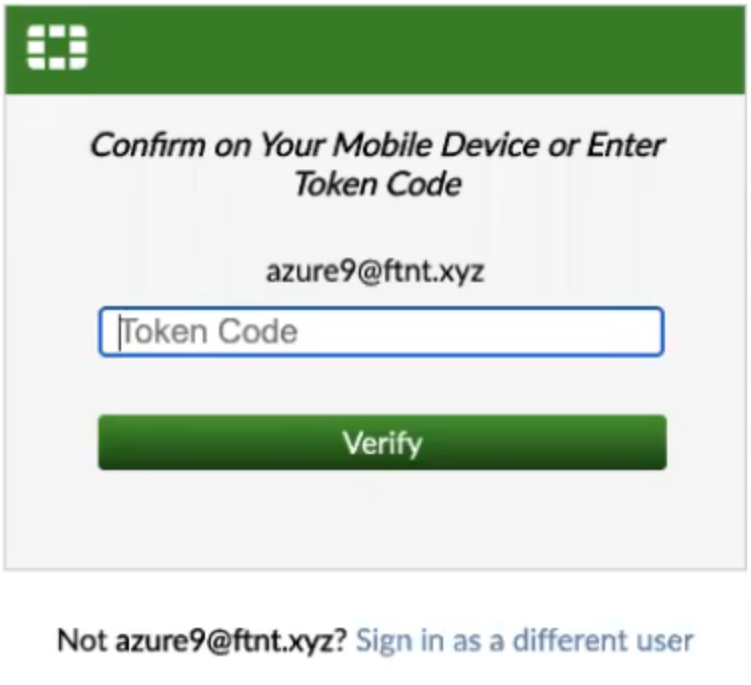
1. Navigate to Office 365 and click *Sign in* or *Switch to a different account*.
2. Enter a user account with domain and click *Sign in*.



3. Authentication is redirected to FortiAuthenticator. Enter your user credentials, and click *Login*.



Enter your 2FA token or approve the access request from your FortiToken push request.

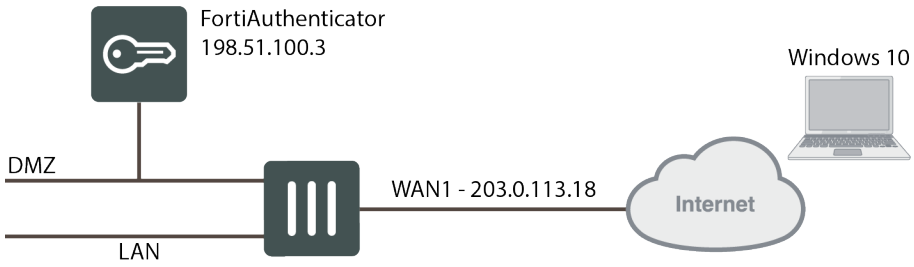


Once approved you are logged in to your Office 365 account.

FortiGate SSL VPN with FortiAuthenticator as the IdP proxy for Azure

This example configuration allows FortiAuthenticator to act as the IdP proxy for Azure authentication to a FortiGate SSL VPN connection. This allows authentication of SSL VPN users against an Azure IdP using two factor authentication with FortiToken by inserting FortiAuthenticator into the authentication flow.

This configuration uses the following topology:

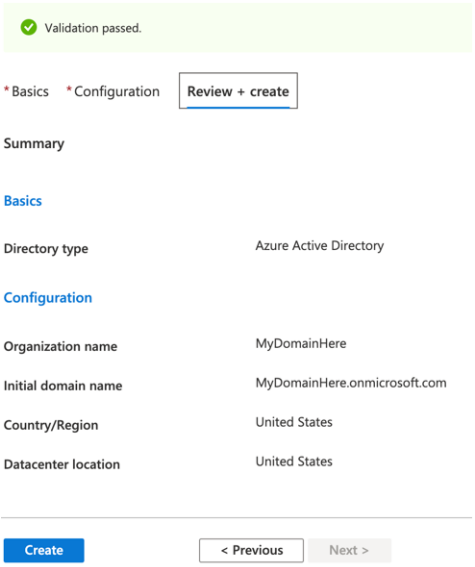


To configure FortiAuthenticator as the IdP proxy for Azure:

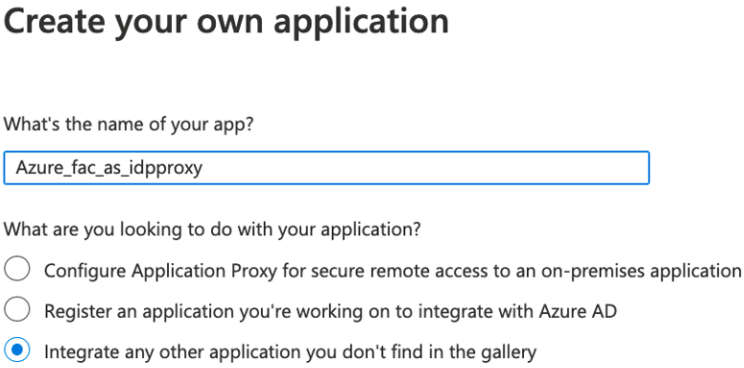
1. Configuring Azure on page 191
2. Configuring FortiAuthenticator on page 194
3. Configuring FortiGate on page 199
4. Results on page 201

Configuring Azure

1. Login to the Azure portal. If you do not yet have a directory or need to create a new one, go to *Azure AD* and click *Create a tenant*.
   Configure the directory with the following settings:
   a. **Select a directory type**: *Azure Active Directory*.
   b. **Organization name**: Enter a name for the organization.
   c. **Initial domain name**: Enter the domain name.
   d. **Country/Region**: Select the relevant country or region.
   e. Click *Create*. The directory will be created after a few minutes. When finished, select the directory in the top-right corner of Azure.

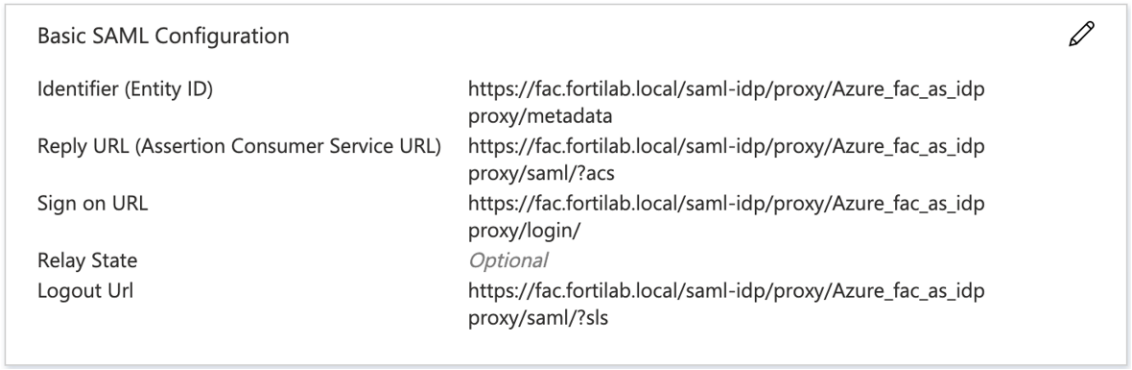


2. Go to *Enterprise Applications*, and select *Create your own application*. Enter a name for your application, for example: `Azure_fac_as_idpproxy`.

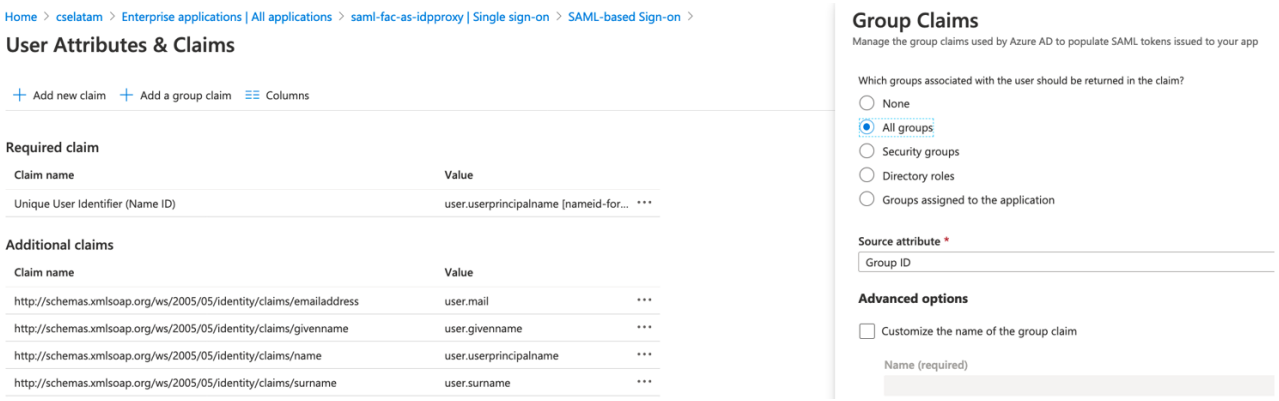


3. Go to the *Single Sign-on* section, select *SAML*, and edit the basic SAML configuration.
   Here you will include information obtained from FortiAuthenticator. In this example, the FortiAuthenticator FQDN is *fac.fortilab.local*, and the name of the server is defined as *Azure_fac_as_idpproxy*. You should adjust these settings

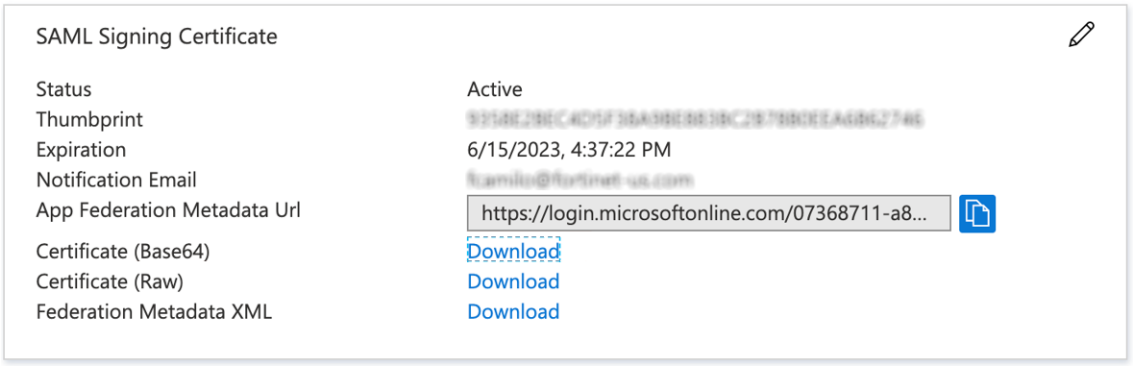
to match your FortiAuthenticator's configuration.



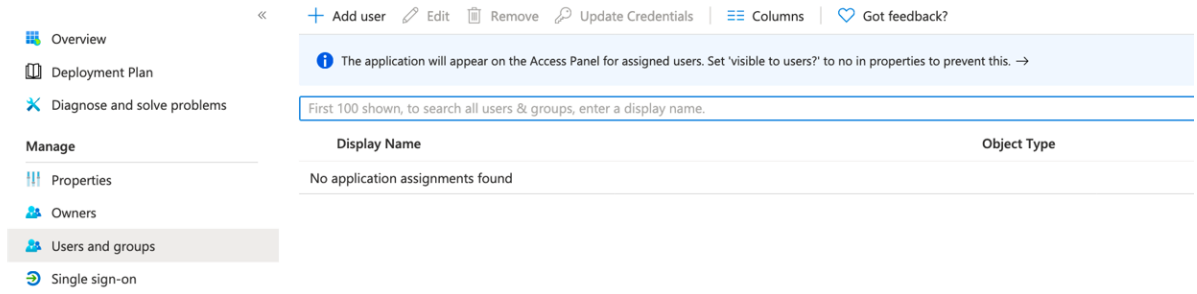
4. Edit the *User Attributes & Claims* section to insert any attributes required for the SAML assertion. In this example, only user groups have been included.
Click the edit icon, and then click *Add a group claim*. Select *All groups*.



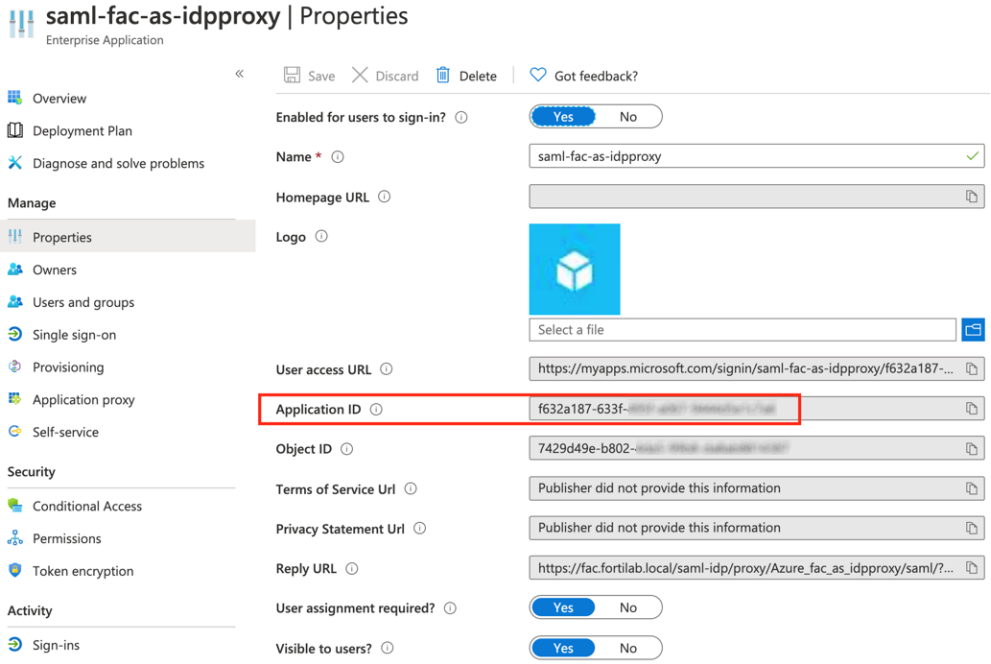
5. Download the certificate file. It will be used later when configuring FortiAuthenticator.



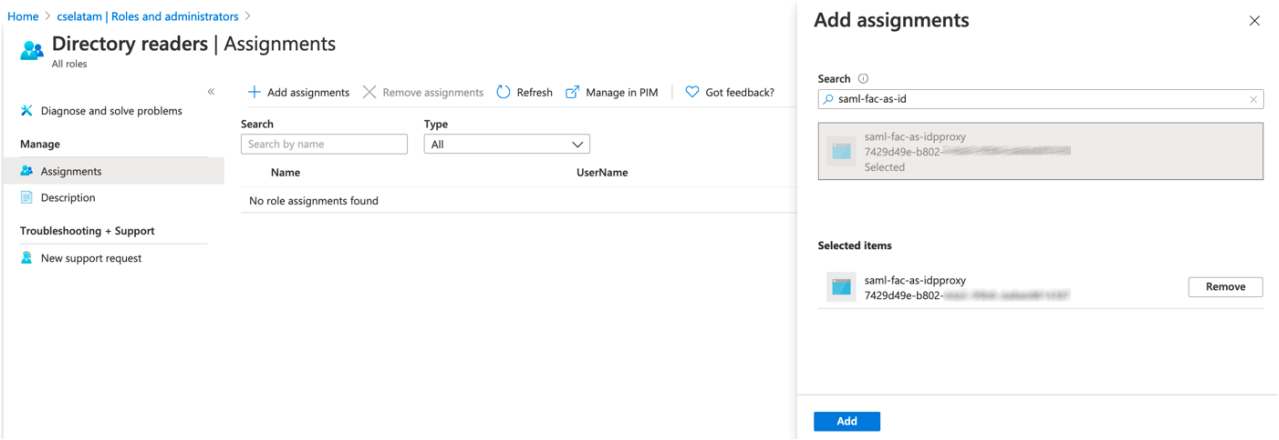
6. Go to *Users and Groups*, and click *Add user*. Include all users that will be able to authenticate using this application.



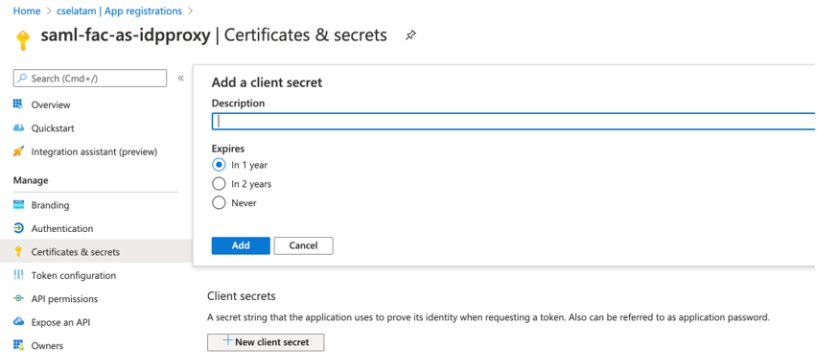
7. Go to *Properties* and get the *Application ID*. This will be required later.



8. From the directory home, select *Roles and Administrators* > *Directory Readers*, and click *Add assignments*. Search for your application name, then select and add it.



9. Finally, create your authentication key. Go to *App Registrations*, click *Certificates & Secrets*, and create a new key.



Before proceeding, make sure to copy the key value. The key is presented only after its creation, and you cannot get this information again later.

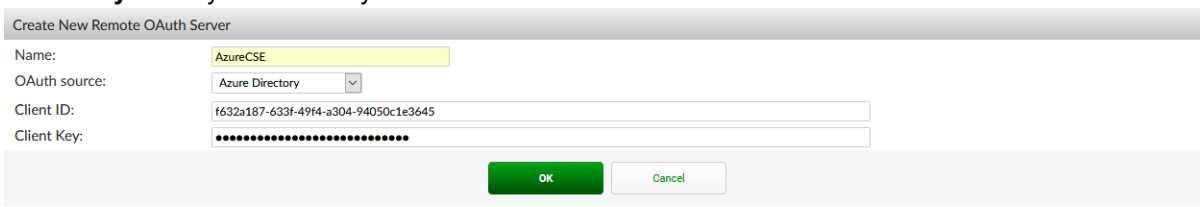
Configuring FortiAuthenticator

Configure the remote servers

A remote OAuth server is used to obtain group membership from Azure AD. Later, a FortiToken can be associated with those users.

To configure the remote OAuth server:

1. Go to *Authentication* > *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Configure the following information:
   - **Name**: Enter a name for your OAuth server, for example: *AzureCSE*.
   - **OAuth source**: *Azure Directory*.
   - **Client ID**: Enter your *Azure Application ID*.
   - **Client Key**: Enter your Azure key.

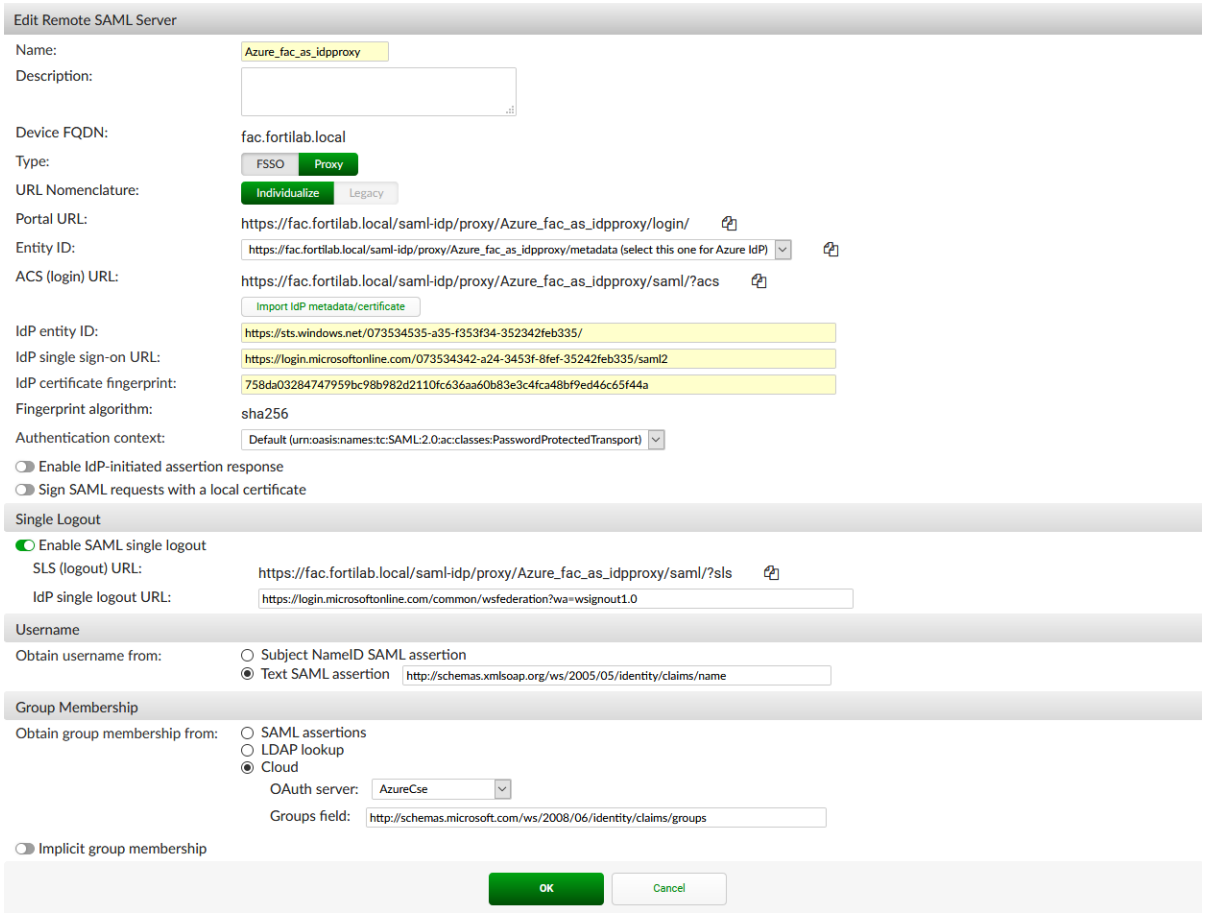


3. Click *OK*.

To configure the remote SAML server:

1. Go to *Authentication* > *Remote Auth. Servers* > *SAML*, and click *Create New*.
2. Under *Remote SAML Server*, configure the following:
   - **Name**: Enter a name for the server. This name must match the server name configured in Azure. In this example, the server name is *Azure_fac_as_idpproxy*.
   - **Type**: *Proxy*.
   - **Entity ID**: Select the Azure IdP option.
   - **Import IdP metadata/certificate**: Import the certificate that you previously exported from Azure.
   - **IdP entity ID**: Enter the *Azure AD Identifier* from your Azure configuration.
   - **IdP single sign-on URL**: Enter the *Login URL* from your Azure configuration.
3. Under *Single Logout*, configure the following:
   - **Enable SAML single logout**: Optionally, you can enable this setting to enable SAML single logout.
   - **IdP single logout URL**: Enter the *Logout URL* from your Azure configuration.
4. Under *Username*, configure the following:
   - **Obtain username from**: Select *Text SAML assertion* and use the configured username claim URL from your Azure configuration.

5. In *Group Membership*, configure the following:
   - **Obtain group membership from**: Select *Cloud* and choose your remote OAuth server. Group membership of a particular user will be retrieved dynamically through OAuth upon authentication.

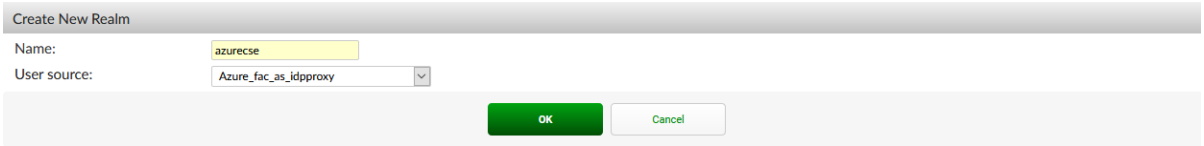


6. Click *OK*.

Configure the SAML IdP settings on FortiAuthenticator

To create the Azure realm:

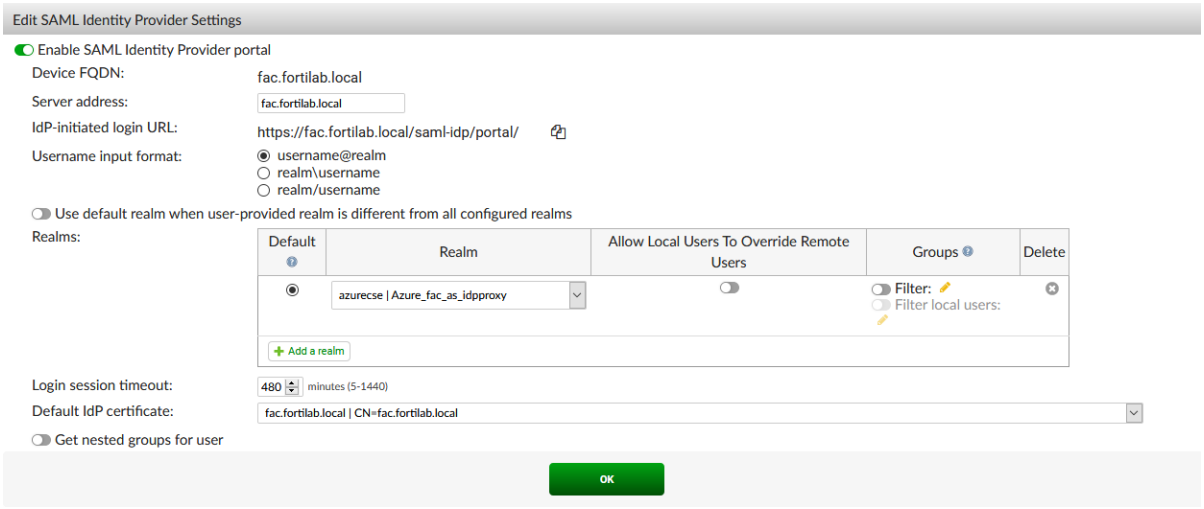
1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Configure the following information:
   a. **Name**: Enter a name for your user realm, for example: *azurecse*
   b. **User source**: Select your remote SAML server as the user source.



3. Click *OK*.

To enable SAML IdP on FortiAuthenticator:

1. Go to *Authentication* > *SAML IdP* > *General*, click *Enable SAML Identity Provider portal*, and configure the following:
   a. **Server address**: Enter the IP or FQDN of your FortiAuthenticator.
   b. **Realms**: Select the SAML realm as the default.
   c. **Default IdP certificate**: Select a default IdP certificate.

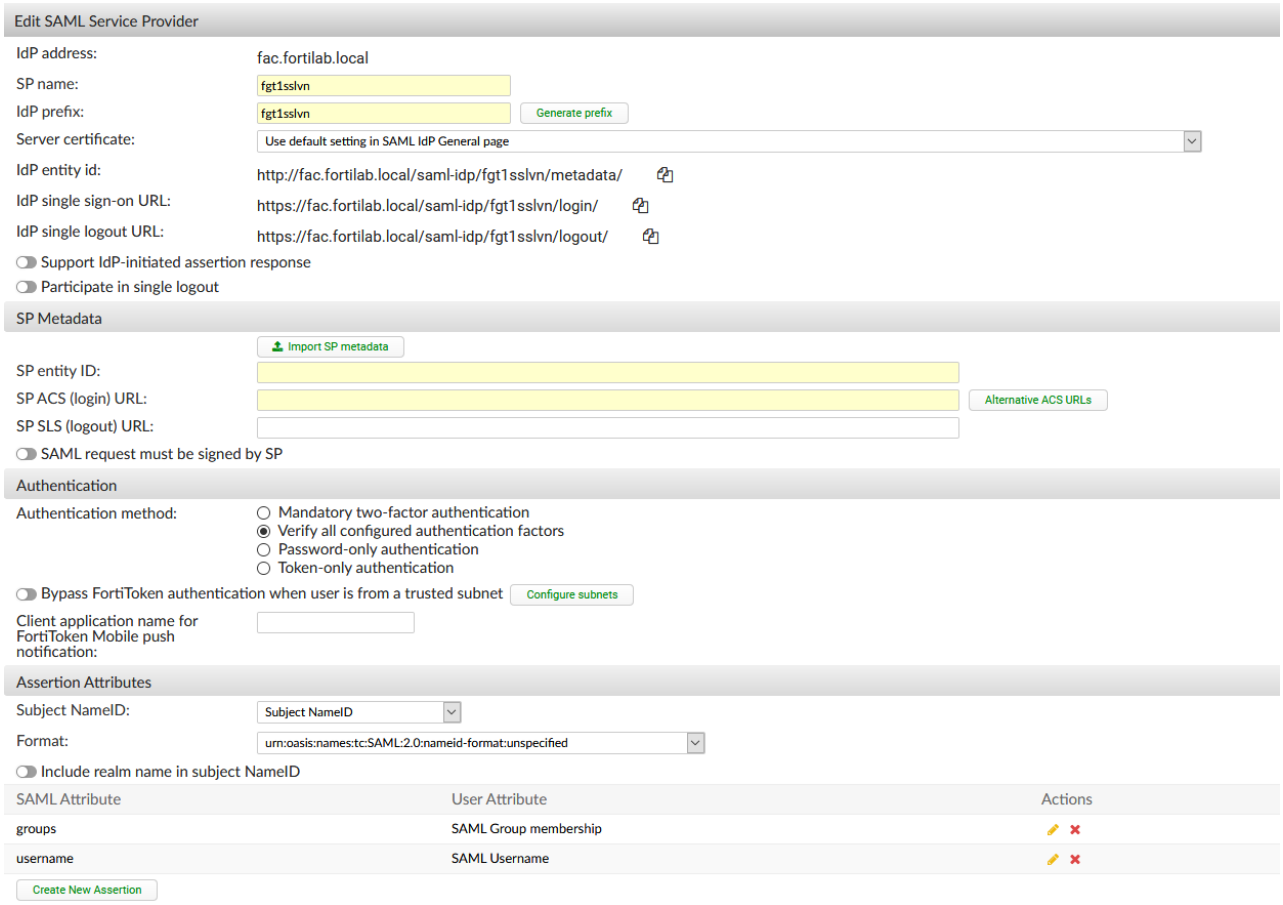


2. Click *OK*.
   You will also need to download your IdP certificate for use later. It can be downloaded from *Certificate Management* > *End Entities*.

To add FortiGate as a SAML service provider:

1. Go to *Authentication* > *SAML IdP* > *Service Providers*, and click *Create New*.
2. Under *Edit SAML Service Provider*, configure the following:
   - **SP name**: Enter a name for this service provider, for example: *fgt1sslvpn*.
   - **IdP prefix**: Enter a custom IdP prefix or click *Generate prefix* to automatically populate this field.
3. Under *Assertion Attributes*, configure the following:
   - **Subject NameID**: *Remote SAML Server* > *Subject NameID*.
   - **Format**: *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified*.
4. Under *SAML Attributes*, add the following attributes. The user and group information will be propagated by the FortiAuthenticator IdP in SAML assertions to FortiGate. These must match with the *user-name* and *group-name* keywords defined for the SAML user. See Configure the SAML user on page 199.
   - Attribute 1: SAML attribute: *groups*, User attribute: *SAML Group membership*.
   - Attribute 2: SAML attribute: *username*, User attribute: *SAML Username*.

5. Click *Save*.



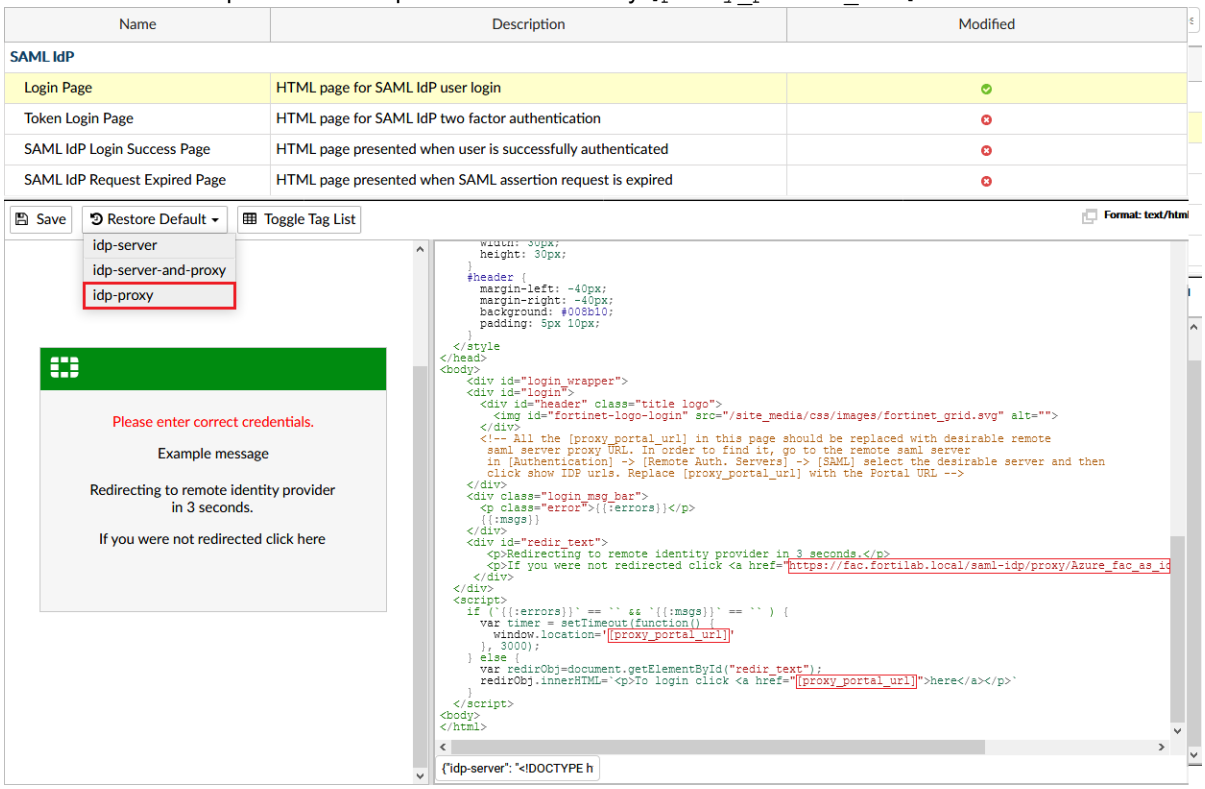
Once the settings have been saved, you will see that additional options are available.

You can return to complete the configuration of the SAML service provider settings on FortiAuthenticator once you have configured your FortiGate SAML user. You will need to enter the *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* from the FortiGate configuration.

To update the SAML replacement message:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*.
2. Select *SAML IdP* > *Login Page*, and then select *idp-proxy* in the *Restore Default* dropdown menu.
   You can now edit the content in the right pane to include the *Portal URL* obtained from your remote SAML server.

The URL must be replaced in three places as indicated by `[proxy_portal_url]` in the text.



3. Click *Save*.

Configure FortiToken

To include tokens in a user's authentication:

1. Go to *Authentication* > *User Management* > *Remote Users*, select *SAML*, and click *Import*.
2. Under *Import Remote SAML Users*, configure the following settings:
   a. **Remote SAML server**: Select your remote SAML server, for example: *Azure_fac_as_idpproxy*.
   b. **Group**: Select *All users* or choose a user group.
3. Click *OK*.
4. Edit an imported user to define the token. Enable *Token-based authentication*, and select your token type.
5. Click *OK*.

Configuring FortiGate

Import the certificate

To import the FortiAuthenticator IdP certificate:

1. Go to *System* > *Certificates*, and click *Import* > *Remote Certificate*.
2. Click *Upload* and select your FortiAuthenticator IdP certificate.
3. Click *OK*.
   FortiGate will choose a name by default. You can rename the certificate for easier management with the following CLI commands:
   ```
   config vpn certificate remote
      rename <DEFAULT_CERT_NAME> to <NEW_CERT_NAME>
   end
   ```

Configure the SAML user

You can now configure a FortiGate SAML user to point to FortiAuthenticator as the IdP.

In this example configuration, the FortiGate SSL VPN link is `https://203.0.113.18:10443`. This can be replaced with the SSL VPN link from your own configuration.

You will also need to adjust the FortiAuthenticator IdP entity ID, login URL, and logout URL to match those configured in your FortiAuthenticator. This information is available on FortiAuthenticator in *Authentication* > *SAML IdP* > *Service Providers*.

Configuring the SAML user must be done through the FortiGate CLI.

To configure a SAML user:

1. In the FortiGate CLI, enter the following commands:
   ```
   config user saml
      edit "fac-samlproxy-sslvpn"
         set cert "Fortinet_Factory"
         set entity-id "https://203.0.113.18:10443/remote/saml/metadata"
         set single-sign-on-url "https://203.0.113.18:10443/remote/saml/login"
         set single-logout-url "https://203.0.113.18:10443/remote/saml/logout"
         set idp-entity-id "http://fac.fortilab.local/saml-idp/fgt1sslvpn/metadata/"
         set idp-single-sign-on-url "https://fac.fortilab.local/saml-
              idp/fgt1sslvpn/login/"
         set idp-single-logout-url "https://fac.fortilab.local/saml-
              idp/fgt1sslvpn/logout/"
         set idp-cert "FAC_IdP"
         set user-name "username"
         set group-name "groups"
      next
   end
   ```

The entity ID, single sign on URL, and single logout URL configured in the FortiGate CLI must now be entered in the FortiAuthenticator service provider configuration.

See To add FortiGate as a SAML service provider: on page 196

The user-name and group-name configured must match what is being returned from FortiAuthenticator in the SAML assertions. See Configure the SAML IdP settings on FortiAuthenticator on page 195.

You can now create a SAML group which includes that user. You can also define the SAML groups that will be allowed to login as this group. In this example, only user that belong to "FGTGroup1" will be allowed to login to the SSL VPN. This can only be done through FortiGate CLI.

To configure a SAML group:

1. In the FortiGate CLI, enter the following commands:

```
config user group
   edit "samlproxy-sslvpn"
      set member "fac-samlproxy-sslvpn"
      config match
         edit 1
            set server-name fac-samlproxy-sslvpn
            set group-name “FGTGroup1”
         next
      end
   next
end
```

Next, increase the remote authentication timeout. This must be set to allow for enough time for the user to authenticate into Azure AD. This can only be done through the FortiGate CLI.

To increase the remote authentication timeout:

1. In the FortiGate CLI, enter the following commands:

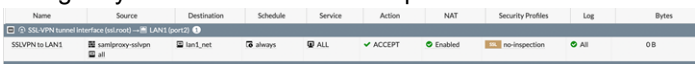
```
config system global
   set remoteauthtimeout 60
end
```

Configure the SSL VPN

You can define a portal for the SAML group in your SSL VPN settings.

To add a portal to your SSL VPN:

1. Go to *VPN* > *SSL-VPN Settings*, and edit your SSL VPN configuration.
2. Under *Authentication/Portal Mapping*, click *Create New*.
3. Configure the following information:
   a. **Users/Groups**: Select the configured user group.
   b. **Portal**: *full-access*.
4. Click *OK* and save your changes to the SSL VPN settings.
5. Configure your SSL VPN rules as required.

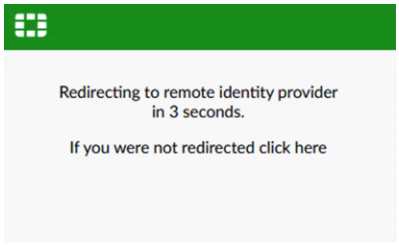


For more information on configuring SSL VPN on FortiGate, see the FortiGate Administration Guide.

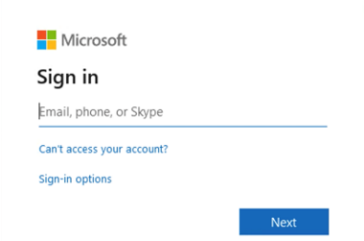
Results

To sign in to your SSL VPN:

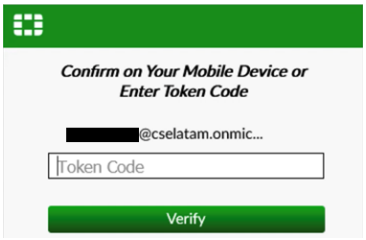
1. Once the user tries to connect to the SSL VPN web portal, FortiGate will redirect the user to FortiAuthenticator. Please note that SAML does not work with the tunnel mode for SSL VPN.



2. The FortiAuthenticator will act as a SAML proxy and forward the request to Azure for authentication.



3. After entering their credentials, if the user has a token assigned they will be requested to enter it for two factor authentication.



4. The user is now connected to the SSL VPN.

Computer Authentication

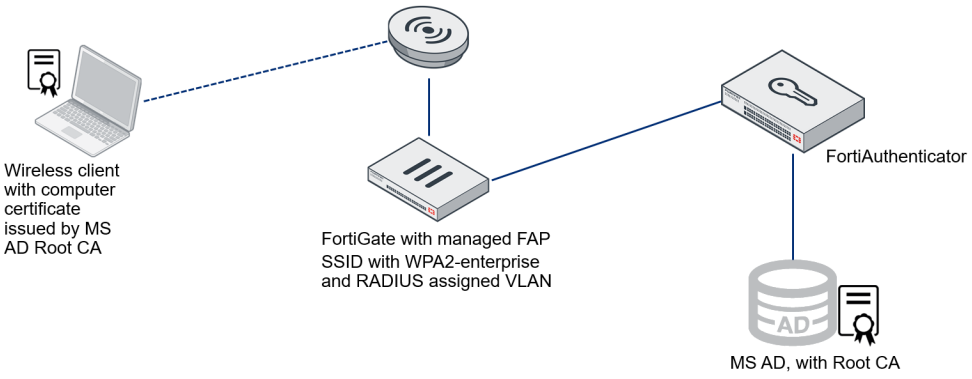
This section describes configuring computer authentication.

Computer authentication using FortiAuthenticator with MS AD Root CA

This example includes the configuration required for computer authentication using FortiAuthenticator with a Microsoft Active Directory Root CA.

This configuration uses the following topology:

- Microsoft Active Directory configured with a Root CA.
- A wireless client with a computer certificate issued by the MS AD Root CA.
- A FortiGate and a managed FortiAP SSID with a WPA2-enterprise and RADIUS assigned VLAN.
- A FortiAuthenticator.



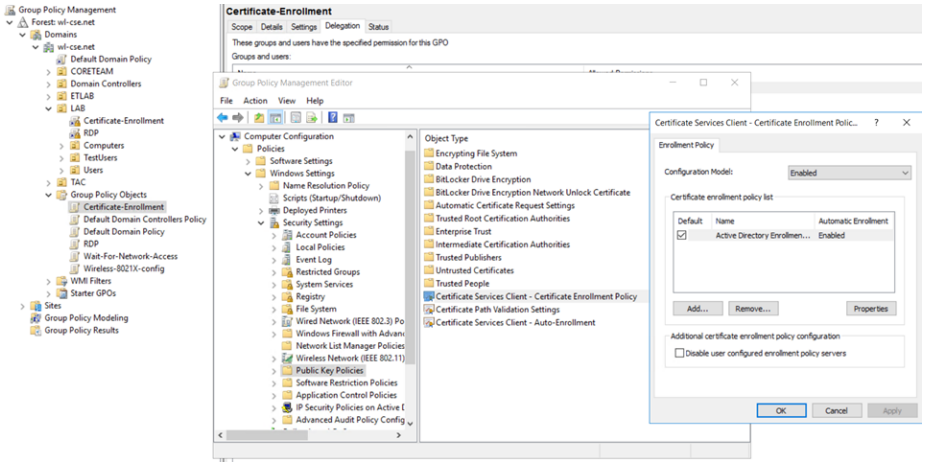
To configure computer authentication using FortiAuthenticator with a Microsoft AD Root CA:

Configure the certificates and Root CA

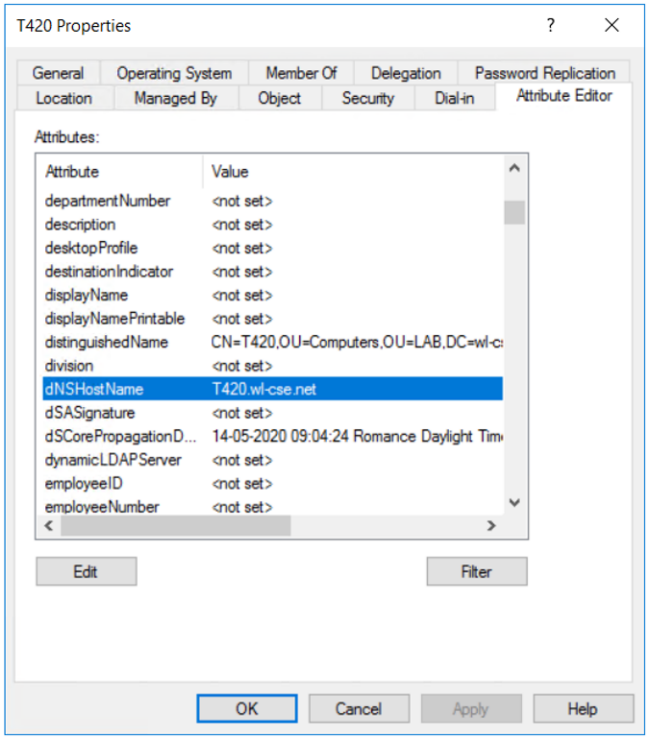
With Microsoft Active Directory as the Root CA, use Group Policy Management to deploy client certificates to domain computers. This is the certificate that will be used to validate RADIUS requests.

To create a computer client certificate:

1. In *Active Directory* > *Group Policy Management*, create a new Group Policy Object (GPO) with settings configured for auto-enrollment.



2. Link the GPO to the OU where the client computers are located.
   The computer account in Active Directory must use the attribute `dNSHostName` with the value of the computer's name. This attribute is used later on FortiAuthenticator when creating the user remote sync rule.



To import the Microsoft AD Root CA as a trusted CA:

1. On the FortiGate, go to *System* > *Certificates*, and click *Import* > *CA Certificate*. Configure the following settings, and click *OK* when complete.
   a. **Type**: *File*.
   b. **Upload**: Click *Upload* and browse to the location of your certificate.

2. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*, and click *Import*. Configure the following settings, and click *OK* when complete.
   a. **Certificate ID**: Enter the certificate ID.
   b. **Certificate**: Click *Upload a file* and browse to the location of your certificate.

Once the Root CA is configured, you can issue certificates from AD to both the FortiGate and the FortiAuthenticator.

Configure LDAP users on FortiAuthenticator

You can now configure the remote LDAP server on FortiAuthenticator to connect to Active Directory, create a user realm and user group, and import the AD users into FortiAuthenticator using a remote user sync rule.

To configure LDAP users on FortiAuthenticator:

1. Configuring the LDAP server on page 204
2. Creating a user realm on page 205
3. Creating a user group on page 206
4. Importing users with a remote user sync rule on page 206

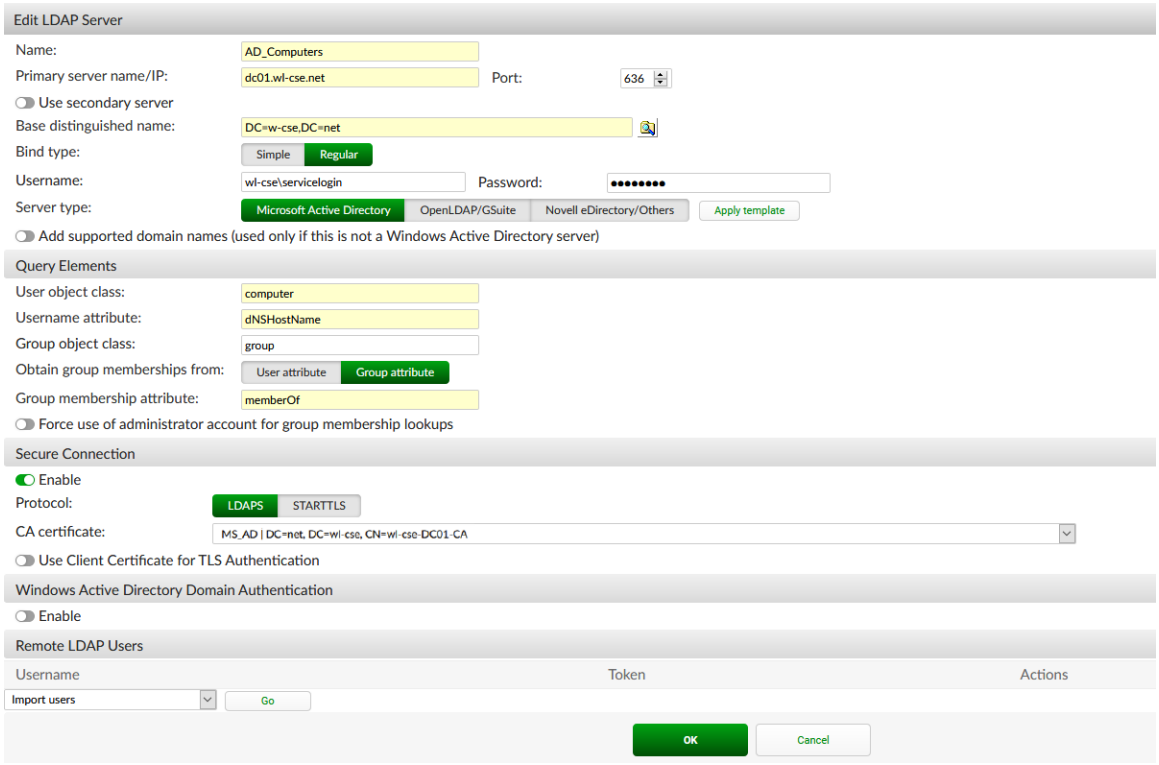
Configuring the LDAP server

Create an LDAP entry for remote lookup of computers with the username attribute as `dNSHostName`.

To configure remote LDAP server on FortiAuthenticator:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. Under *Create New LDAP Server*, set the following:
   a. **Name**: Enter the server name, for example: `AD_Computers`.
   b. **Primary server name/IP**: Enter the LDAP server name, for example: `dc01.wl-cse.net` using *Port* 636.
   c. **Base distinguished name**: Enter the base distinguished name, for example: `DC=wl-cse,DC=net`.
   d. **Bind type**: *Regular*.
   Enter the username and password for your LDAP user.
3. Under *Query Elements*, set the following:
   a. **User object class**: `computer`.
   b. **Username attribute**: `dNShostName`.
   c. **Group object class**: `group`.
   d. **Obtain group memberships from**: *Group attribute*.
   e. **Group membership attribute**: `memberOf`.

4. Enable *Secure Connection*, and set the following:
   a. **Protocol**: *LDAPS*.
   b. **CA certificate**: Select the CA certificate you previously configured.



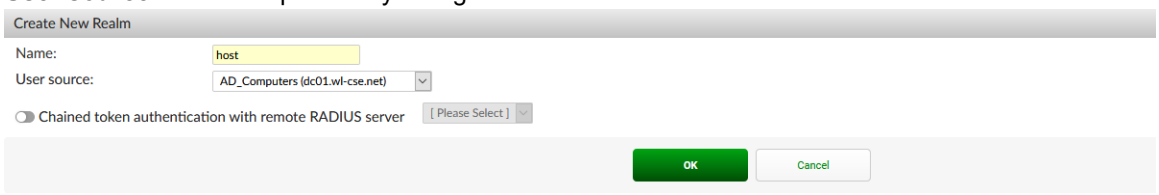
5. Click *OK*.

Creating a user realm

Create a user realm for the users (computers) from your remote LDAP. This realm is used later when configuring RADIUS authentication.

To create a user realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the realm, for example: `host`.
   b. **User source**: Select the previously configured remote LDAP server.



3. Click *OK*.

Creating a user group

Create a user group for the users (computers) from your remote LDAP.

To create a remote LDAP user group:

1. Go to *Authentication* > *User Management* > *User Groups*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the LDAP group, for example: `AD_LAB_PC`.
   b. **Type**: *Remote LDAP*.
   c. **User retrieval**: Set a list of imported remote LDAP users.
   d. **Remote LDAP**: Select the previously configured remote LDAP server, for example *AD_Computers*.
   e. **LDAP users**: Add your chosen LDAP users to the *Selected LDAP Users* pane.
3. Click *OK*.

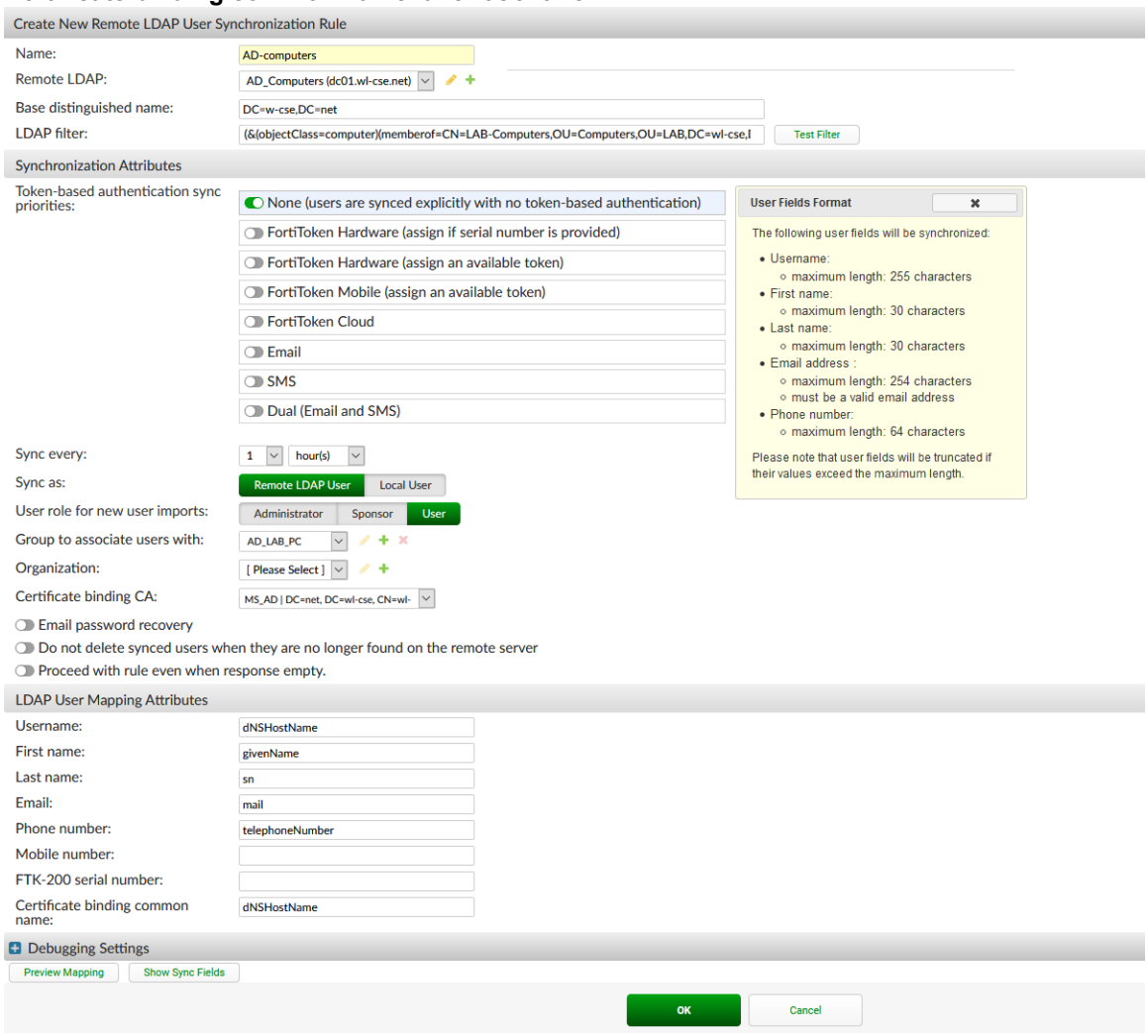
Importing users with a remote user sync rule

Create the user sync rule to import your users (computers) into FortiAuthenticator. You can configure this rule with an LDAP filter to match specific groups in Active Directory. For the LDAP *username* and *certificate binding common name*, use `dNSHostName`. This must match the CN of the actual issued certificate.

To configure a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*, and click *Create New*.
2. Under *Edit Remote LDAP User Synchronization Rule*, set the following:
   a. **Name**: Enter a name for the rule, for example: `AD-computers`.
   b. **Remote LDAP**: Select the remote LDAP server you previously configured.
   c. **Base distinguished name**: Enter your base distinguished name, for example: `DC=wl-cse,DC=net`.
   d. **LDAP filter**: Select the LDAP filter which matches your specific group in Active Directory, for example: `(&(objectClass=computer)(memberof=CN=LAB-Computers,OU=Computers,OU=LAB,DC=wl-cse,DC=net))`.
3. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: Select *None*.
   b. **Sync every**: Select the sync frequency based on your preferences, for example: *1 hour(s)*.
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.
   e. **Group to associate users with**: Select your remote LDAP user group.
   f. **Certificate binding CA**: Select your CA for certificate binding.

4. Under *LDAP User Mapping Attributes*, set the following:
   a. **Username**: `dNSHostName`.
   b. **Certificate binding common name**: `dNSHostName`.



5. Click *OK*.

Once the user sync rule has been created, run it to import your user (computer) account, and then verify the user was successfully created in *Authentication* > *User Management* > *Remote Users* and that the certificate binding is in place.

Configure RADIUS authentication

You can now configure RADIUS authentication between the FortiAuthenticator and FortiGate.

To configure RADIUS authentication:

1. Adding RADIUS attributes on page 208
2. Configuring the RADIUS client on page 208
3. Configuring the EAP server certificate on page 209

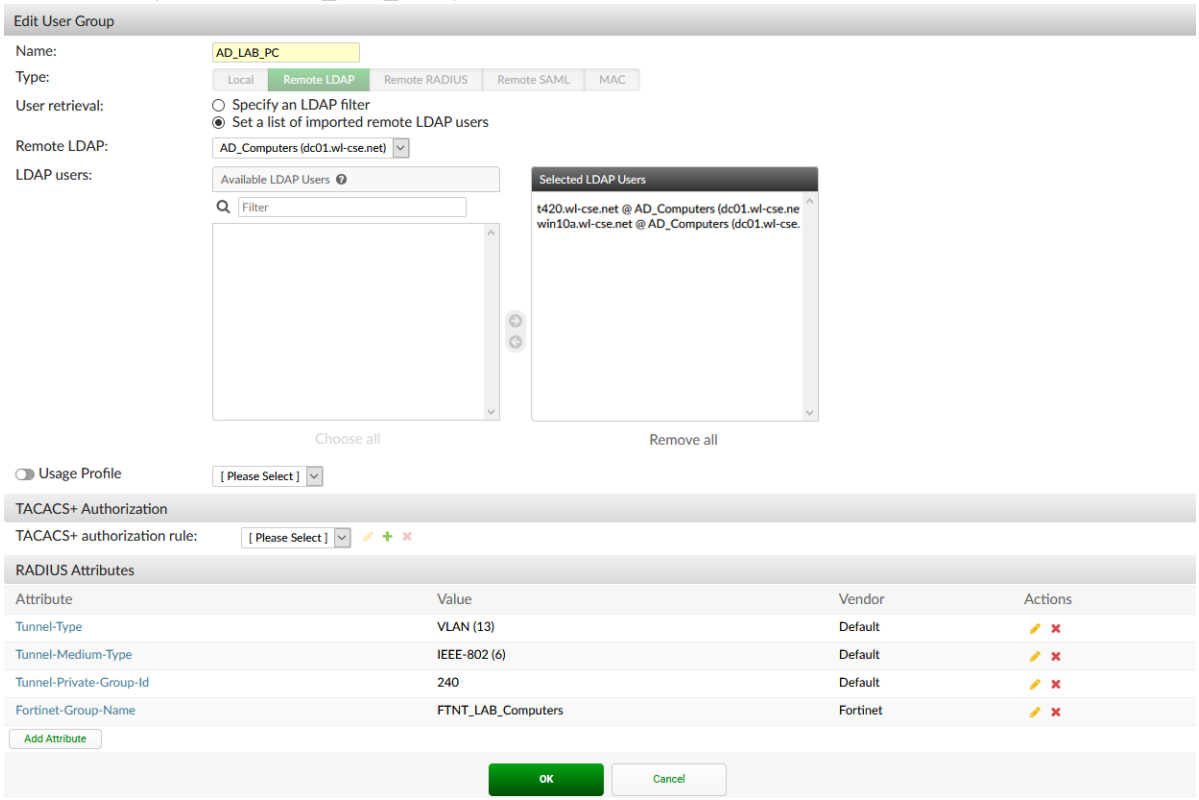
4. Creating a RADIUS policy on page 209
5. Configuring the RADIUS server on FortiGate on page 211

Adding RADIUS attributes

RADIUS attributes can be added to the previously configured LDAP user group.

To add RADIUS attributes to the LDAP user group:

1. Go to *Authentication* > *User Management* > *User Groups*, and edit the user group associated with the remote LDAP users.
2. Under *RADIUS Attributes*, add the RADIUS attributes required by your configuration. In this example, the following attributes are required:
   - Tunnel-Type: VLAN.
   - Tunnel-Medium-Type: IEEE-802.
   - Tunnel-Private-Group-Id: 240.
   - Fortinet-Group-Name: FTNT_LAB_Computers.

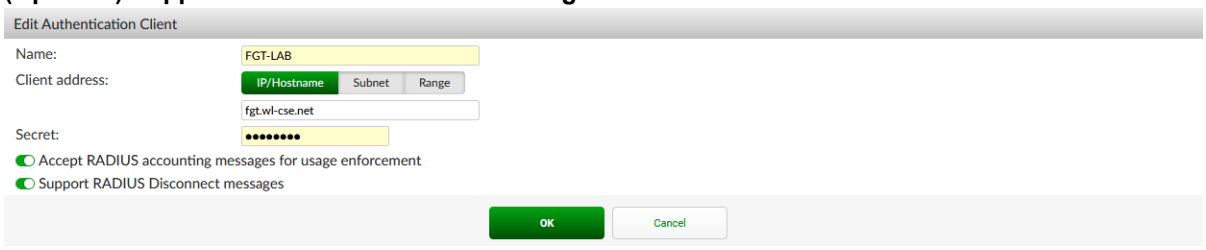


Configuring the RADIUS client

To configure RADIUS authentication using FortiAuthenticator, the FortiGate must be configured as a RADIUS client.

To configure the RADIUS client settings:

1. Go to *Authentication* > *RADIUS Service* > *Clients*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the RADIUS client, for example: `FGT-LAB`.
   b. **Client address**: Select IP/Hostname, and enter your RADIUS client's IP or hostname, for example: `fgt.wl-cse.net`.
   c. **Secret**: Enter a shared secret. This will also be used to configure RADIUS settings on FortiGate.
   d. **(Optional) Accept RADIUS accounting messages for usage enforcement**: *Enabled*.
   e. **(Optional) Support RADIUS Disconnect messages**: *Enabled*.



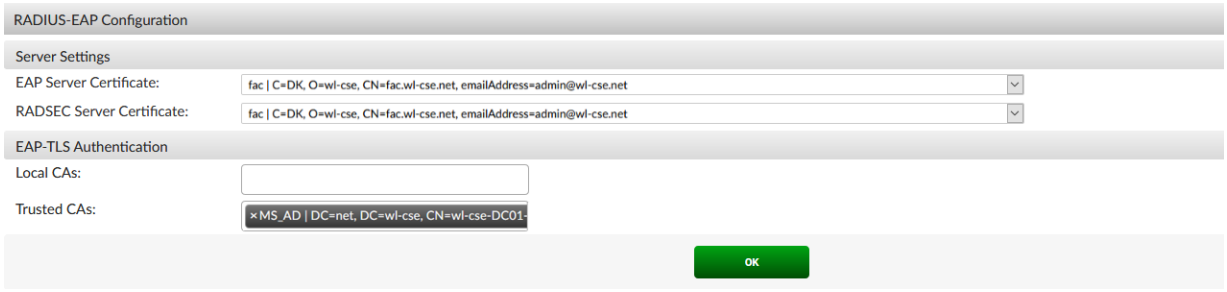
3. Click *OK*.

Configuring the EAP server certificate

In order to use EAP, you must specify the certificate used for FortiAuthenticator in the RADIUS-EAP configuration settings.

To configure the RADIUS certificate for EAP-TLS:

1. Go to *Authentication* > *RADIUS Service* > *Certificates*.
2. Specify the *EAP Server Certificate* and the *Trusted CA* from Active Directory that you previously configured.



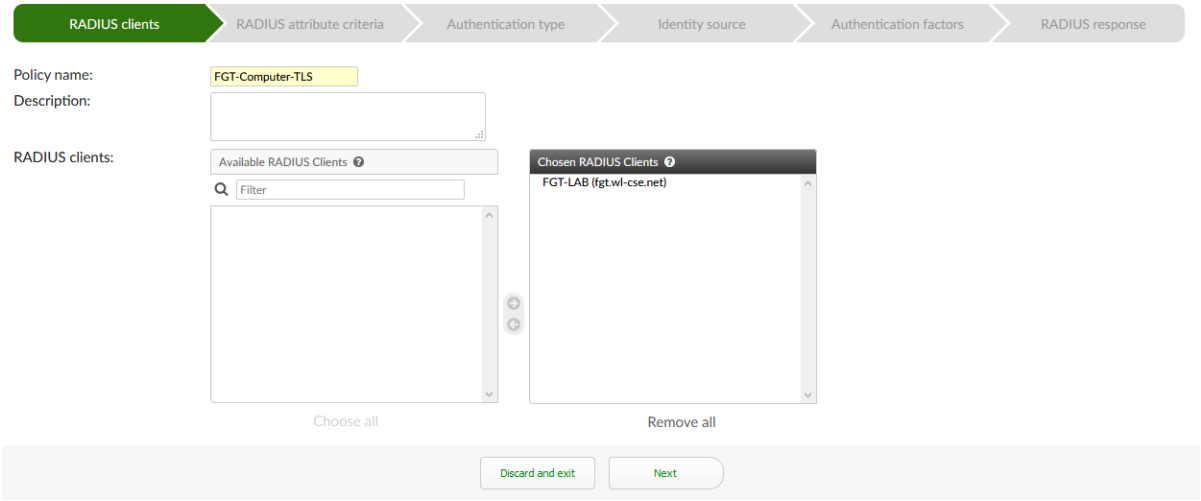
3. Click *OK*.

Creating a RADIUS policy

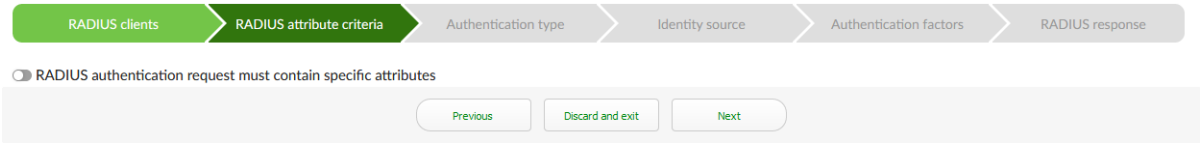
A RADIUS policy must be configured in order to allow RADIUS authentication for the selected client.

To create a RADIUS policy:

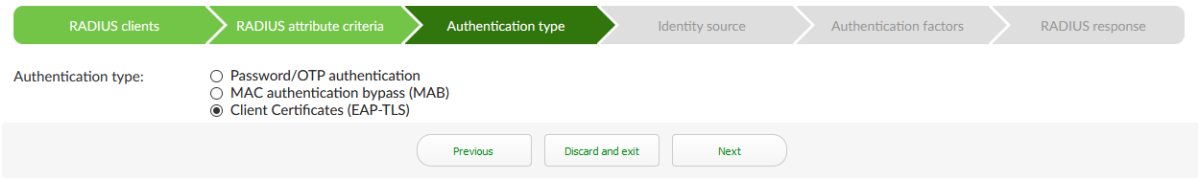
1. Go to *Authentication* > *RADIUS Service* > *Policies*, and click *Create New*.
2. Under RADIUS clients, configure the following, and click *Next*.
   a. **Policy name**: Enter a name for this policy, for example: *FGT-Computer-TLS*.
   b. **RADIUS clients**: Add the previously configured FortiGate RADIUS client to the *Chosen RADIUS Clients* section.



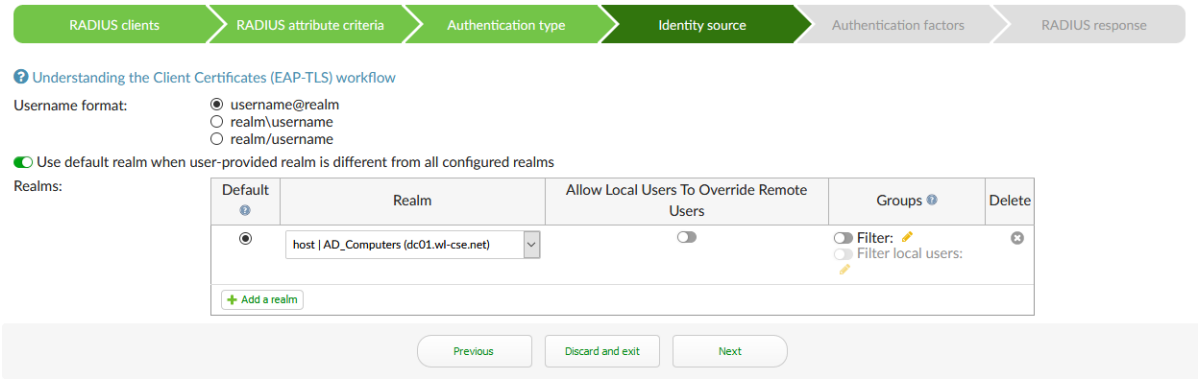
3. Under *RADIUS attribute criteria*, click *Next*.



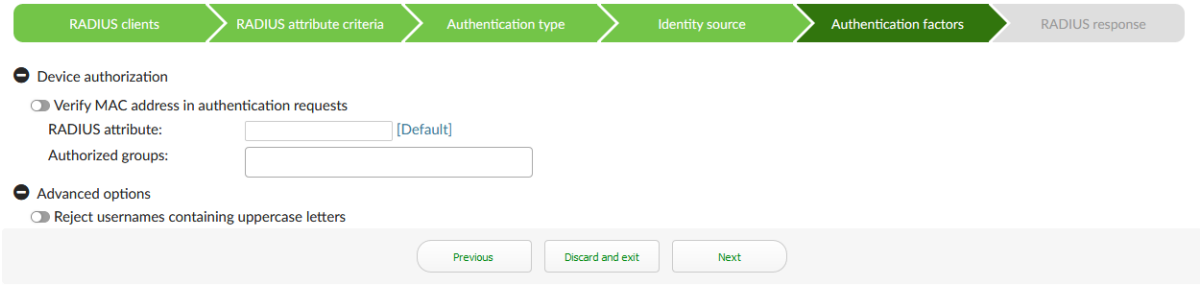
4. Under *Authentication type*, choose *Client Certificates (EAP-TLS)*, and click *Next*.



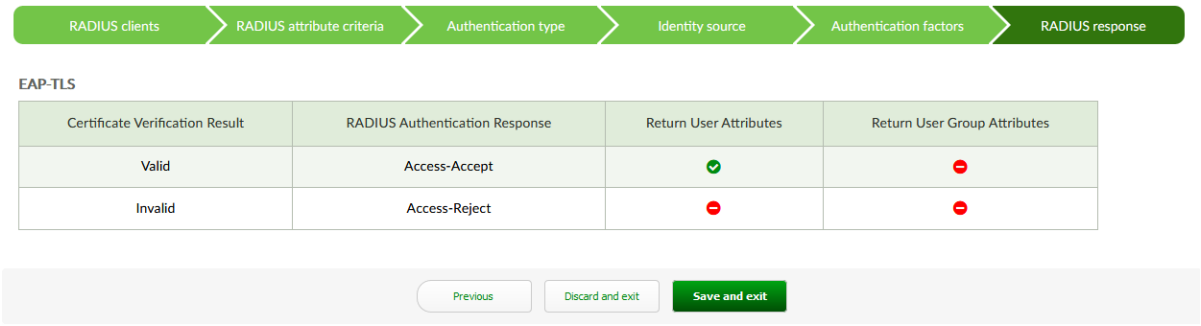
5. Under *Identity source*, configure the following, and click *Next*.
   a. **Username format**: Select your preferred username format, for example: *realm\username*.
   b. **Realms**: In the *Realms* table, select your AD realm.
   You can additionally apply a group filter if required.



6. Under *Authentication factors*, click *Next*.



7. Under *RADIUS response*, click *Save and exit*.



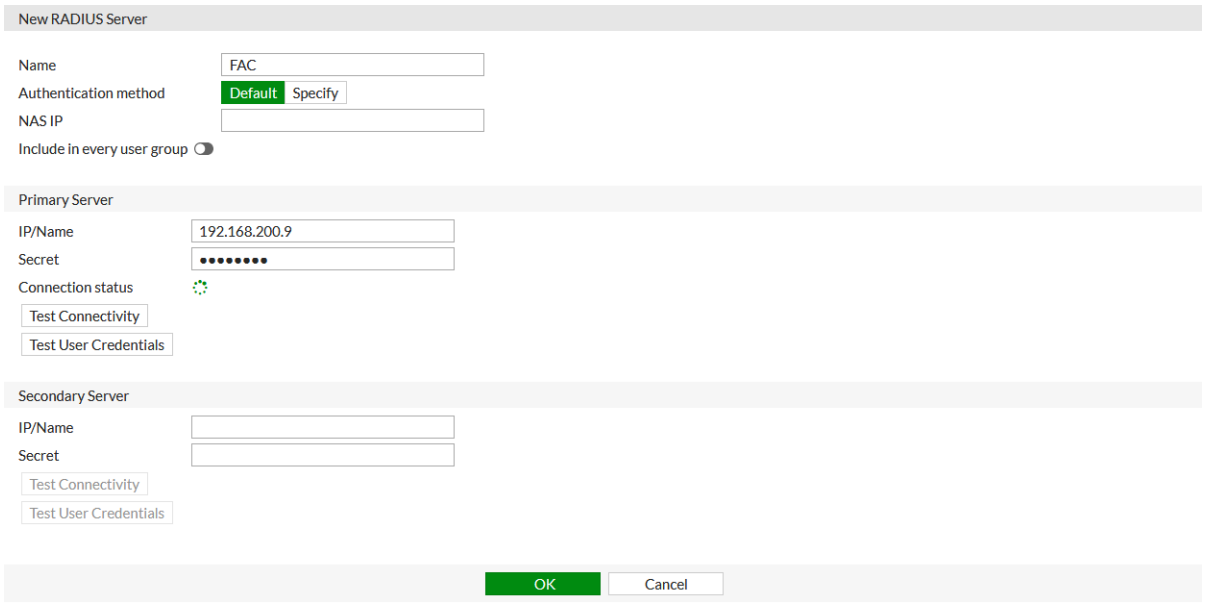
Configuring the RADIUS server on FortiGate

Finally, you can configure the RADIUS server settings (FortiAuthenticator) on FortiGate.

To configure the RADIUS server on FortiGate:

1. On FortiGate, go to *User & Authentication* > *RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
   a. **Name**: Enter a name for the RADIUS server, for example: *FAC*.
   b. **Authentication method**: *Default*.

3. Under *Primary Server*, set the following:
   a. **IP/Name**: Enter the IP address of the FortiAuthenticator.
   b. **Secret**: Enter the RADIUS server secret created on FortiAuthenticator.



4. Click *OK*.

Configure the SSID and interface objects

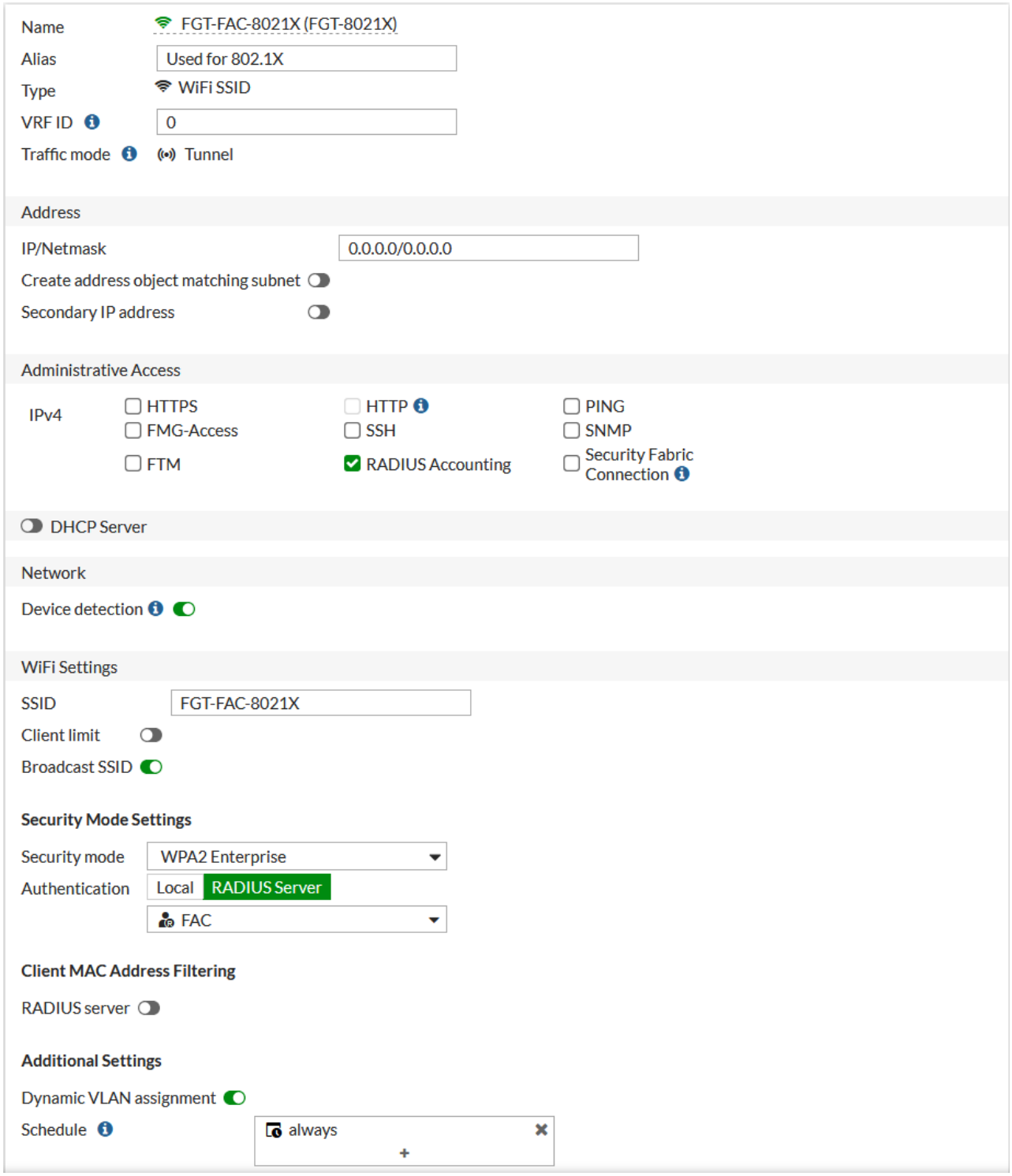
To configure the SSID and interface objects:

1. Creating the SSID on page 213
2. Creating interfaces on page 214

Creating the SSID

To create an SSID with dynamic VLAN assignment:

1. On FortiGate, go to *WiFi & Switch Controller* > *SSID*, and click *Create New* > *SSID*.
2. Create a new SSID with *Dynamic VLAN assignment* enabled under *Additional Settings*.

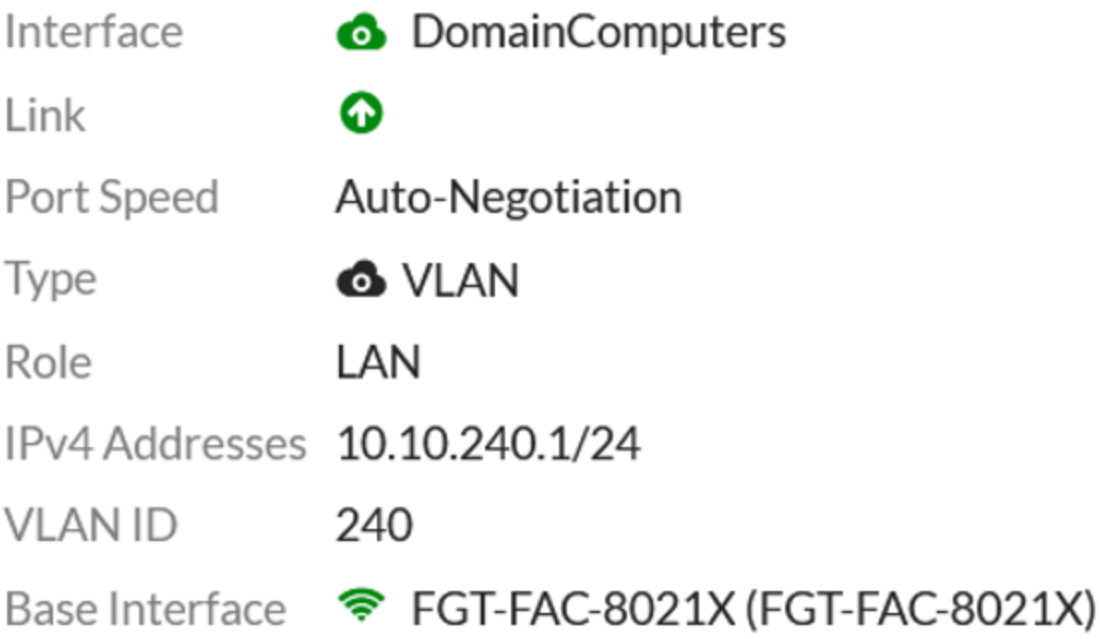


Creating interfaces

You can now create interfaces as required.

To create additional interfaces:

1. Go to *Network* > *Interfaces*, and click *Create New* > *Interface*.
2. Configure your VLAN interface. In this example, the DomainComputers VLAN is created with the following settings:
   a. **Name**: DomainComputers.
   b. **Type**: *VLAN*.
   c. **Interface**: The configured SSID, FGT-FAC-8021X (FGT-FAC-8032X).
   d. **VLAN ID**: 240
   e. **Role**: LAN.

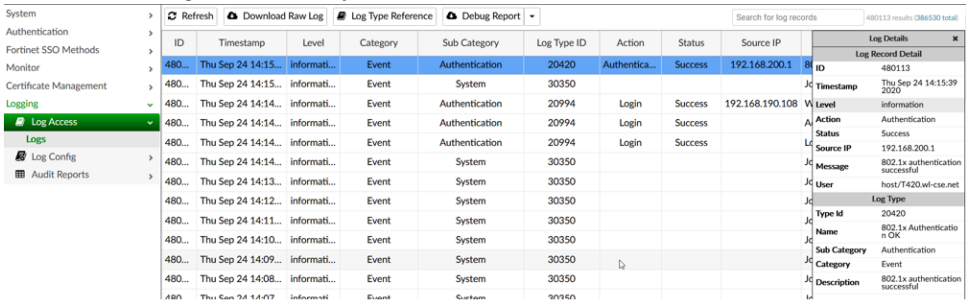


Results

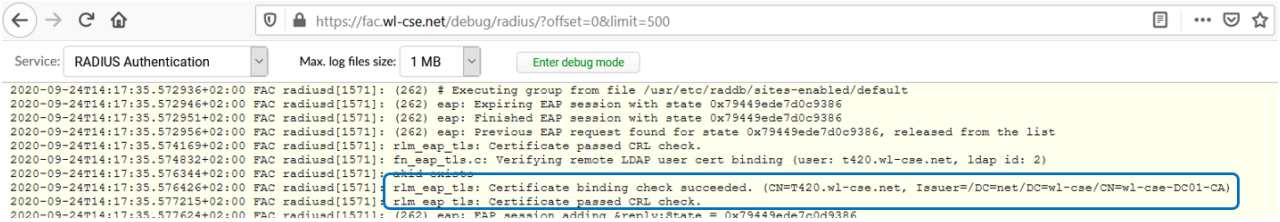
Once the configuration is complete, you should now be able to authenticate your computer using FortiAuthenticator with a Microsoft AD Root CA.

To confirm computer authentication is working as intended:

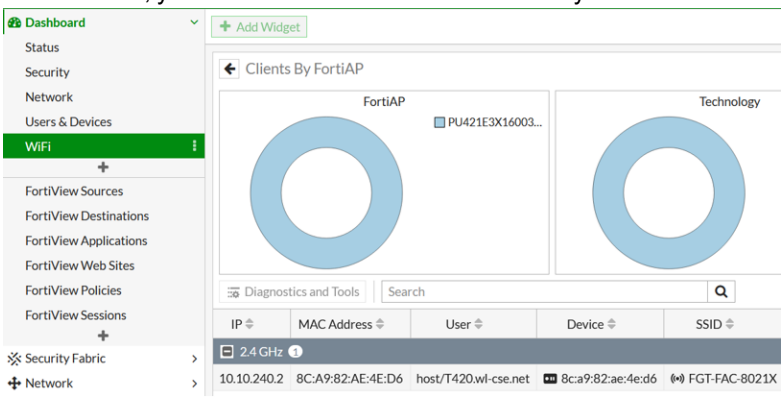
1. When connecting to the client, you can see *Authentication Success* in the FortiAuthenticator logs.



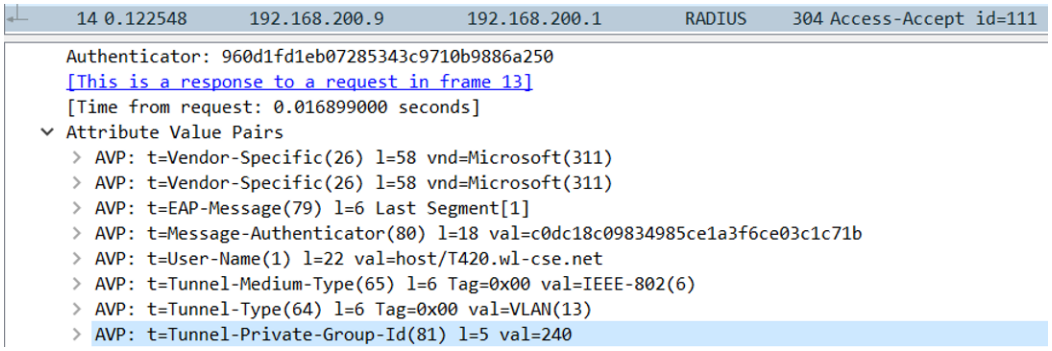
2. When reviewing the debug logs, you can see that certificate binding check has passed.



3. On FortiGate, you can see that the client successfully connected:



4. Packet capture shows the RADIUS-Accept message, including the VLAN 240.



WiFi onboarding using FortiAuthenticator Smart Connect

This example demonstrates how to configure WiFi onboarding using FortiAuthenticator Smart Connect with either Google G Suite or Microsoft Azure.

This configuration assumes that you have already configured your FortiAuthenticator following the initial configuration steps available within the FortiAuthenticator Administration Guide. FortiAuthenticator must be version 6.1.1 or higher.

Before starting, you should already have the following available:

- A registered domain name and functional DNS. This example uses fortixpert.com.
- A publicly signed wildcard certificate for your domain (for example *.fortixpert.com used to sign MS Azure DS Secure LDAP Connector).
- A publicly signed host/server certificate for FortiAuthenticator.
- An active Google G Suite Enterprise or MS Azure subscription, depending on your chosen configuration.
  - Please note: Secure LDAP is not supported using G Suite Business or G Suite Basic subscriptions.
  - An active MS Azure subscription requires AD Directory Services to be provisioned in order to support Secure LDAP.
- Have the appropriate Fortinet infrastructure in place, for example, Fortigate running FOS 6.2.4GA+, FortiSwitch running 6.2.4GA+, FortiAP/FortiAP-U running latest GA and FortiAuthenticator 6.1.1 and above.

To configure WiFi onboarding using Smart Connect:

1. Initial settings on FortiAuthenticator on page 216
2. Select either the G Suite or Azure configuration:
   a. Option A - WiFi onboarding with Smart Connect and G Suite on page 220
   b. Option B - WiFi onboarding with Smart Connect and Azure on page 230
3. FortiGate configuration on page 238
4. Results on page 249

Initial settings on FortiAuthenticator

To set up the initial configuration on FortiAuthenticator:

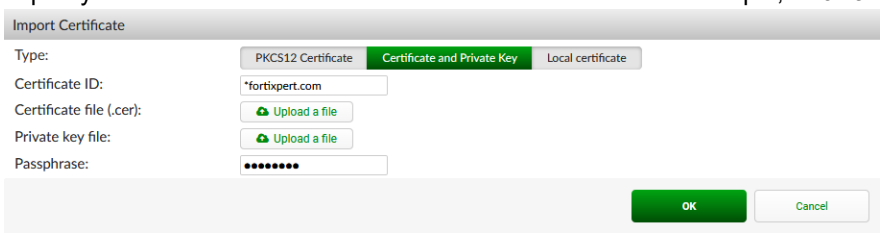
1. Install certificates on page 216
2. Configure the RADIUS client settings on page 218
3. Configure the local root CA on page 218
4. Configure the EAP server certificate and CA for EAP-TLS on page 219

Install certificates

To install a wildcard certificate on FortiAuthenticator:

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CA*.
   Import a trusted root/intermediate public CA certificate in order to support your wildcard certificate.

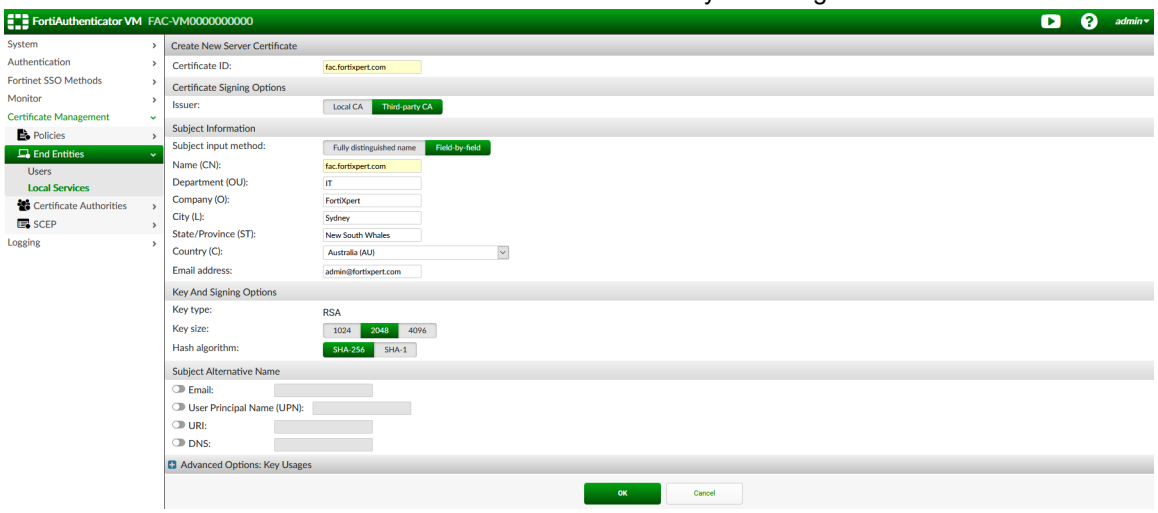
2. In *Certificate Management* > *End Entities* > *Local Services*, click *Import*, select *Certificate and Private Key*, and import your domain wildcard certificate as *domainname. For example, `*fortixpert.com`.



To generate a Certificate Signing Request (optional):

The following steps are optional and can be done if the server certificate matching the FortiAuthenticator FQDN is not yet available.

1. In *Certificate Management* > *End Entities* > *Local Services*, select the *Create New* button.
   Configure the following settings:
   a. Under *Create New Server Certificate*, set the *Certificate ID* to your certificate name, for example, fac.fortixpert.com.
   b. Under *Subject Information*, configure the *Name*, *Department*, *Company*, *City*, *State/Province*, *Country* and *Email Address* for your certificate.
   c. (Optional) If you are using a self-signed certificate on FortiAuthenticator, add a Subject Alternative Name (SAN) matching the FQDN under *Subject Alternative Name*.
   d. (Optional) Under *Advanced Options: Key Usages*, choose all *Key Usages* and *Extended Key Usages*.
   e. All other fields can be left in their default state. Click *OK* to save your changes.



2. Export the pending CSR by selecting the pending entry and then clicking *Export Certificate*. Use the downloaded `certificate-name.csr` file to obtain a certificate from a public CA.
3. Import the signed certificate file from the public CA by selecting *Import* and uploading the `certificatename.cer` file.

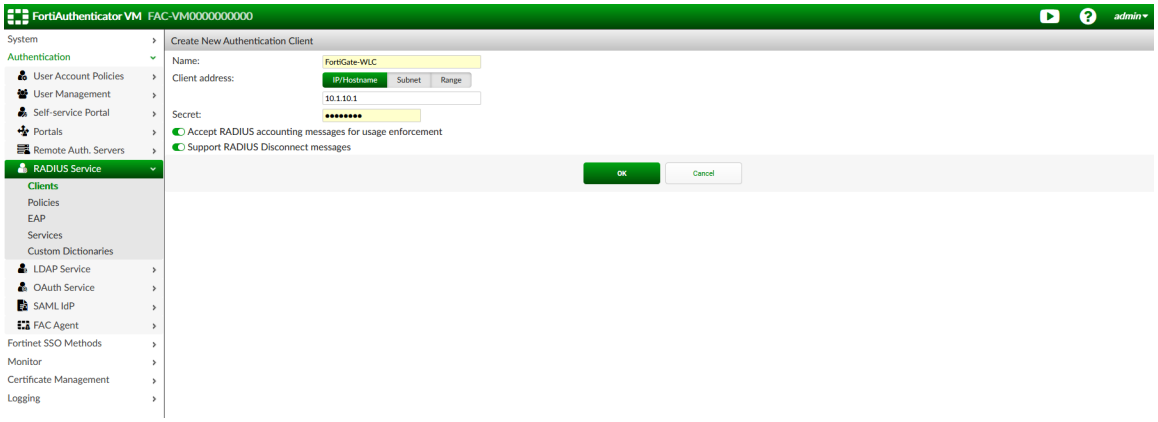
To install local service certificates:

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CA*.
   Upload the trusted root/intermediate public CA certificates in order to support your host/server certificate.
2. Under *Certificate Management* > *End Entities* > *Local Services*, *Import* your publicly signed host/server certificate matching the FQDN (i.e. fac.fortixpert.com) along with the matching private key.
3. Under *System* > *Administration* > *System Access* > *GUI Access*, configure the following:
   a. For *HTTPS Certificate*, select the server certificate matching the device FQDN from the dropdown box.
   b. For *CA Certificate*, select the Root CA certificate that was used to sign the host/server certificate selected above.
4. Select *OK*.

Configure the RADIUS client settings

To configure the RADIUS client:

1. Add the FortiAuthenticator host record to your local DNS server.
   If you are using FortiGate as the DNS server, this can be set under *Network* > *DNS Servers* on FortiGate.
2. Under *System* > *Dashboard* > *Status*, edit and set the hostname and FQDN for FortiAuthenticator so that it matches the DNS host record.
3. In *Authentication* > *RADIUS Service* > *Clients*, add the wireless controller, in this example FortiGate, as a new RADIUS client.
   Enter the *Name* and *IP/Hostname* of the wireless controller, and create a *Secret*.
4. Click *OK*.

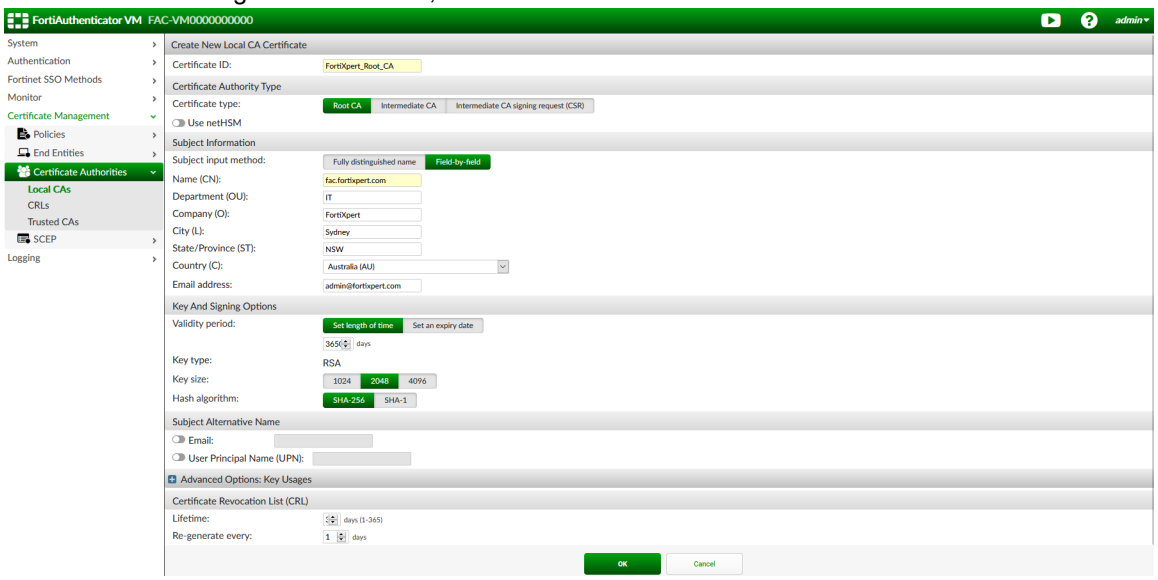


Configure the local root CA

You can now configure a local CA on FortiAuthenticator. This will be used to generate client certificates for authentication via EAP-TLS.

To configure the Local Root CA:

1. In *Certificate Management* > *Certificate Authorities* > *Local CAs*, select *Create New*.
2. Configure the following settings:
   a. Set the *Certificate ID* to the Local_Root_CA_Name.
   b. In *Certificate Authority Type*, set the *Certificate Type* to *Root CA*.
   c. In *Subject Information*, configure the *Name*, *Department*, *Company*, *City*, *State/Province*, *Country*, and *Email address* for your certificate.
   d. In *Advanced Options* > *Key Usages*, choose *all* Key Usages and Extended Key Usages.
3. Leave all other settings as their default, and click *OK*.

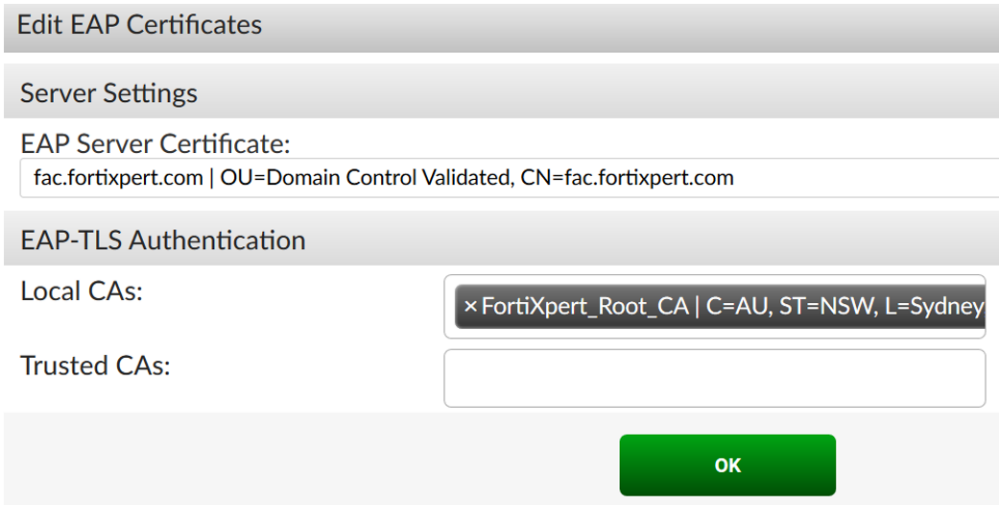


Configure the EAP server certificate and CA for EAP-TLS

To set an EAP Server Certificate and CA for EAP-TLS:

1. Go to *Authentication* > *RADIUS Service* > *Certificates*.
2. In *Server Settings* > *EAP Server Certificate*, select the publicly signed certificate matching the FortiAuthenticator FQDN (e.g. fac.fortixpert.com).

3. In *EAP-TLS Authentication* > *Local CAs*, select the local CA (e.g. FortiXpert_Root_CA).



4. Click *OK*.

Option A - WiFi onboarding with Smart Connect and G Suite

This section outlines how to configure the FortiAuthenticator to communicate with G Suite via Secure Lightweight Directory Access Protocol.

To configure WiFi Onboarding with G Suite:

1. Configure G Suite LDAPS Integration on page 220
2. Configure Smart Connect and the captive portal on page 226
3. Configure RADIUS settings on FortiAuthenticator on page 229

Configure G Suite LDAPS Integration

Here you will configure FortiAuthenticator to communicate with Google G Suite via Secure Lightweight Directory Access Protocol.

To configure FortiAuthenticator and G Suite LDAPS integration:

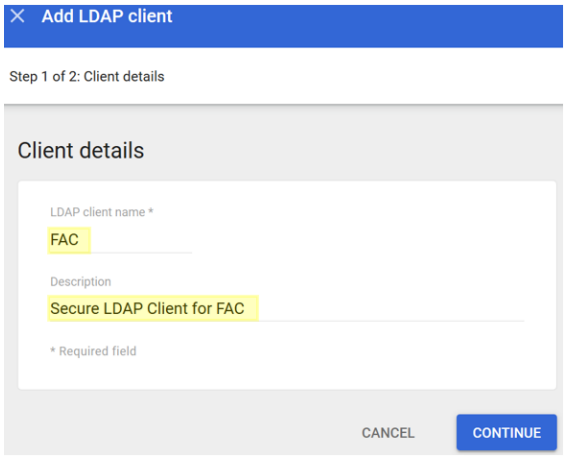
1. Provision the LDAP connector in G Suite on page 221
2. Configure certificates on FortiAuthenticator on page 223
3. Configure the remote LDAP server and users on page 224

Provision the LDAP connector in G Suite

To provision the LDAP connector in G Suite:

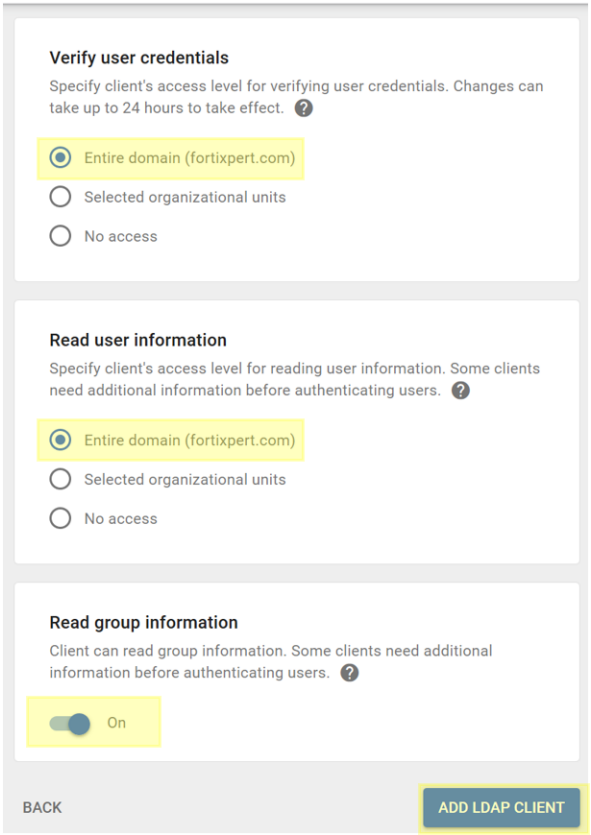
Configure FortiAuthenticator to communicate with Google G Suite via Secure Lightweight Directory Access Protocol (LDAPS).

1. Login to the G Suite admin console using a G Suite admin account.
2. Click the Apps icon, then select *LDAP* and *Add Client*.
3. In *Add LDAP Client Step 1*, configure the following settings:
   a. **Name**:Enter a name, for example *FAC*.
   b. **Description**: Enter a description, for example *Secure LDAP Client for FAC*.



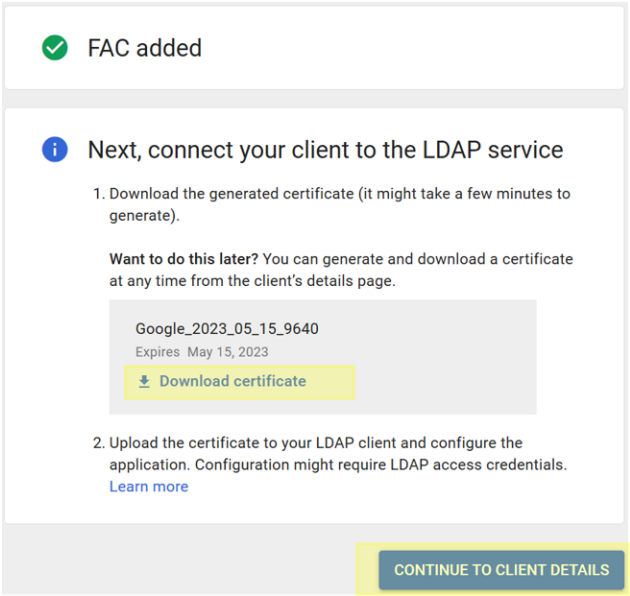
4. Under Add LDAP Client Step 2, configure the following settings:
   a. **Verify User Credentials**: *Entire domain*.
   b. **Read user information**: *Entire domain*.
   c. **Read Group Information**: *On*.

5. Click *Add LDAP Client*.



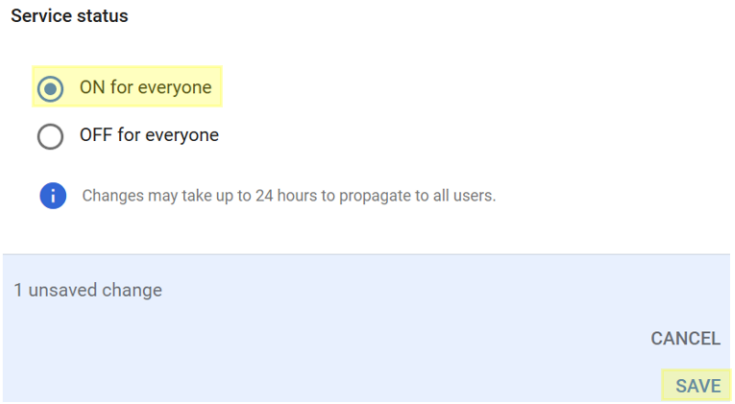
You will now be prompted to connect your client to the LDAP service.

6. Click *Download Certificate* and save the ZIP file.



Unzip the certificate file to a local folder. Contained within will be a public certificate along with a private key.

7. Select *Continue to Client Details*. Select Service status and change the status to *On*.



8. Click *Save*.

Configure certificates on FortiAuthenticator

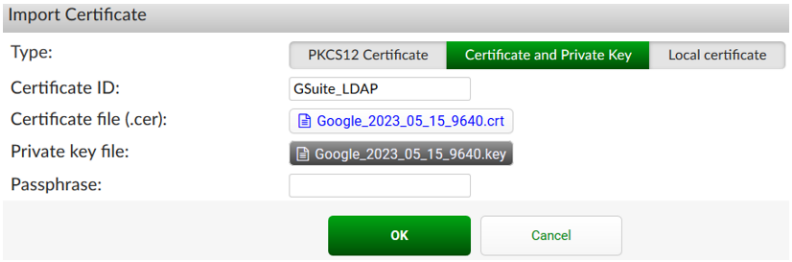
To download Google Root CA Certificate:

1. Open a new Internet browser and navigate to https://pki.goog.
2. Under *Root CAs* in the *Repository* tab, download the *GS Root R2* certificate in the DER format. The file will be called *GSR2.crt*.

To import the Google Certificates into FortiAuthenticator:

1. In FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*, and click *Import*.
2. Enter a *Certificate ID* and then upload the Google Root CA certificate previously downloaded.

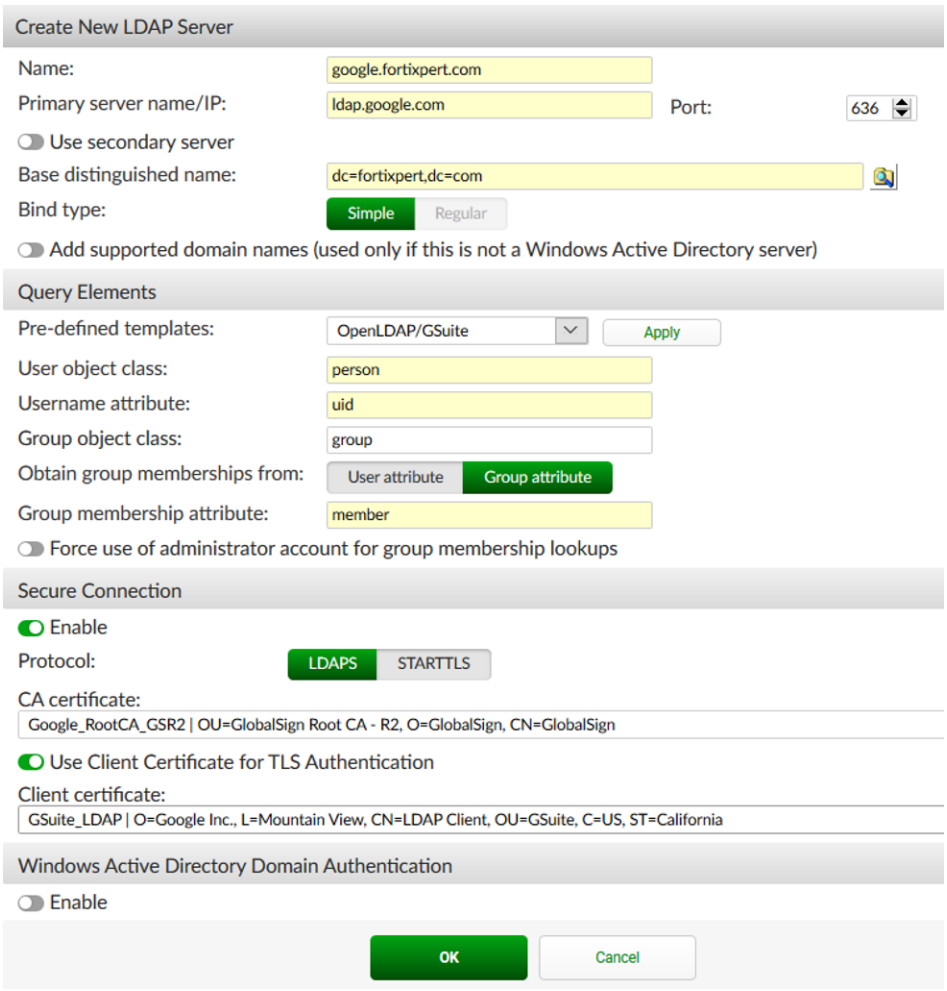
3. Go to *Certificate Management* > *End Entities* > *Local Services*, and click *Import*.
4. Under *Import Certificate* , select *Certificate and Private Key* as the *Type*.
Enter a *Certificate ID*, and select the *Certificate file* and *Private key file* from the file you unzipped previously. A *Passphrase* is not required. Click *OK*.



Configure the remote LDAP server and users

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. Under *Create New LDAP Server*, set the following:
   a. **Name**: Enter a name for the remote LDAP server, for example *google.fortixpert.com*.
   b. **Primary server name/IP**: *ldap.google.com*.
   c. **Base distinguished name**: Enter the base LDAP search directory, for example the G Suite domain: *dc=fortixpert,dc=com*.
   d. **Bind type**: *Simple*.
3. Under *Query Elements*, set the following:
   a. **Pre-defined templates**: Select *OpenLDAP/G Suite* from the dropdown box, and click *Apply*.
4. Under *Secure Connection*, enable the secure connection function, and set the following:
   a. **Protocol**: *LDAPS*.
   b. **CA Certificate**: Select the *Google_RootCA_GSR2* certificate from the dropdown box.
   c. **Use Client Certificate for TLS Authentication**: *Enabled*.
   d. **Client certificate**: Select the *G Suite_LDAP* client certificate from the dropdown box.
5. At the top of the page under Base distinguished name, select the directory lookup icon.
   Once the LDAPS connection is established you'll see the Directory of Groups and Users within G Suite. Select *OK*.



6. Select *OK* again to save the LDAP server settings.

To import remote user accounts:

1. Go to *Authentication* > *User Management* > *Remote Users*, and confirm that *LDAP* is selected at the top right of the page.
2. Click *Import*.
3. Under *Import Remote LDAP Users*, set the following:
   a. **Remote** LDAP server: Select your connector bound to ldap.google.com from the dropdown box.
   b. **Action**: *Import Users*.
4. Click *Go*. A list of all the users within your G Suite directory will be displayed.
5. Select the users you want to be able to connect to the wireless network using their G Suite account, and select *OK* to import the relevant user accounts.
6. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: *None*.
   b. **Sync every**: Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.
7. Leave all other settings in their default state, and click *OK*.

To create a new realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Configure the following settings:
   a. **Name**: Enter a name for your realm, for example fortixpert.com.
   b. **User source**: Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a captive portal using Smart Connect authenticating against Google G Suite.

To configure Smart Connect and portals on FortiAuthenticator:

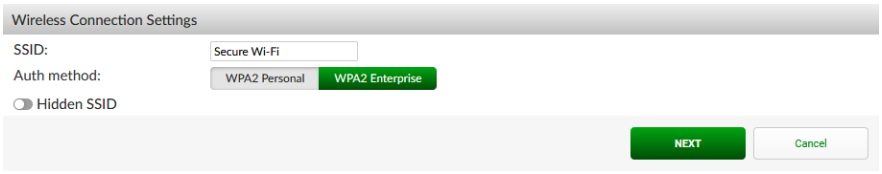
1. Create the Smart Connect profile on page 226
2. Create the captive portal on page 227
3. Create the self-service portal policy on page 228

Create the Smart Connect profile

To create Smart Connect profiles:

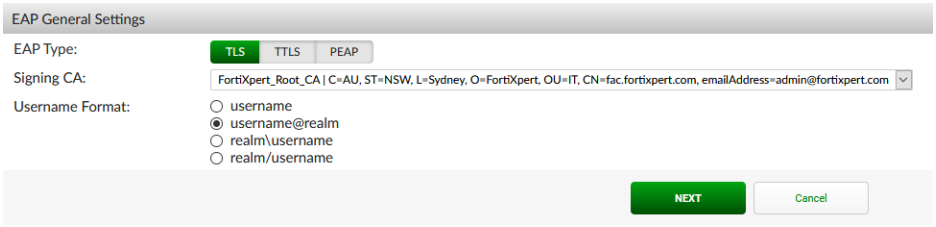
1. Go to *Authentication* > *Portals* > *Smart Connect Profiles*, and click *Create New*.
2. Under *General Information*, enter a name for the profile, and click *Next*.

3. Under *Wireless Connection Settings*, set the following and then click *Next*.
   a. **SSID**: Enter your SSID name, for example Secure Wi-Fi.
   b. **Auth method**: *WPA2 Enterprise*.
   c. **Hidden SSID**: *Disabled*.

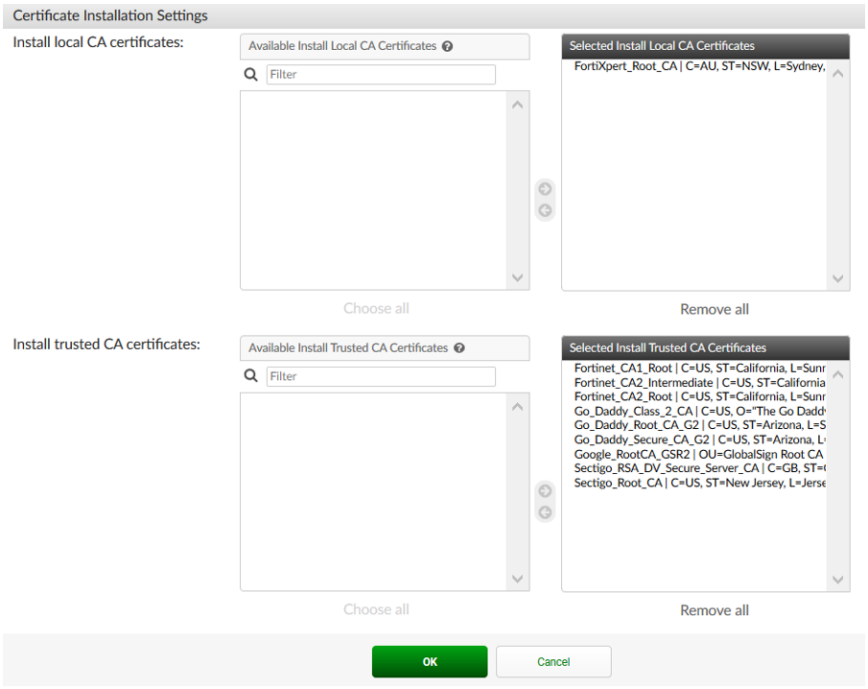


4. Under *EAP General Settings*, set the following and then click *Next*.
   a. **EAP Type**: *TLS*.
   b. **Signing CA**: Select the local Root CA configured earlier.

c. **Username Format**: Select your preference, for example *username@realm*.



5. Under *Certificate Installation Settings*, set the following and then click *OK*.
   a. **Install local CA certificates**: Choose to install the local Root_CA certificate.
   b. **Install trusted CA certificates**: Choose to install any certificate that is required for all relevant certificate chains to be fully trusted.



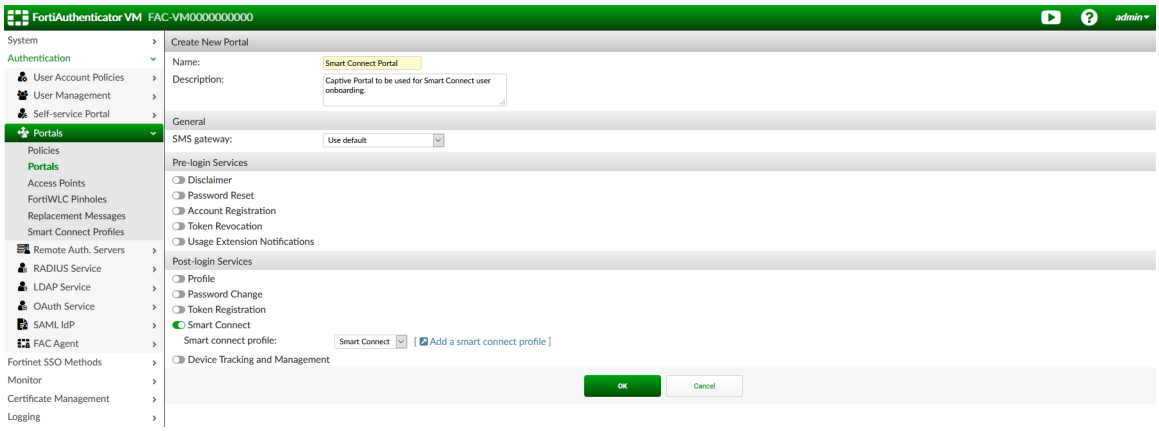
6. Select *OK* to complete the setup of the Smart Connect profile.

Create the captive portal

To create a captive portal:

1. Go to *Authentication* > *Portals* > *Portals*, and click *Create New*.
2. Under *Create New Portal*, enter a name and optional description for the portal.
3. Under *Post-login services*, enable *Smart Connect* and select the previously configured Smart Connect profile from the dropdown.

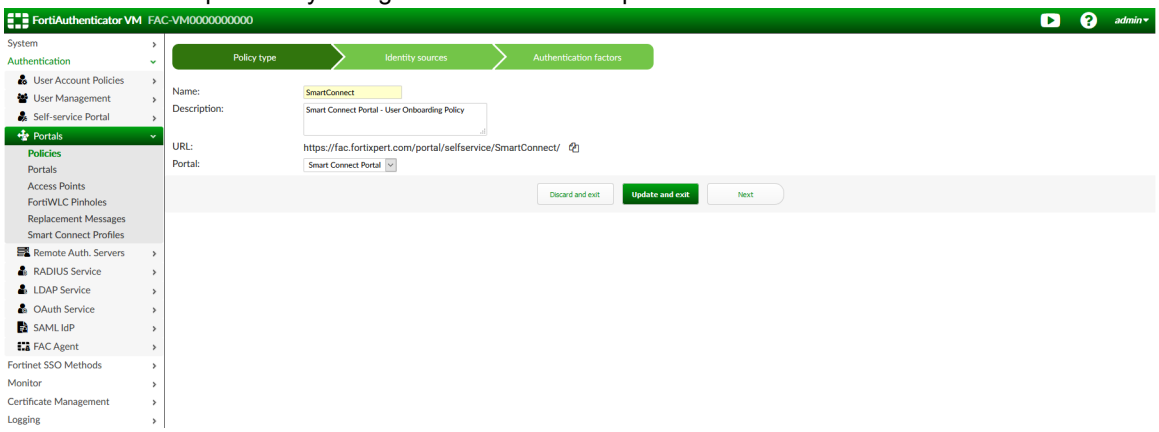
4. Select *OK*.



Create the self-service portal policy

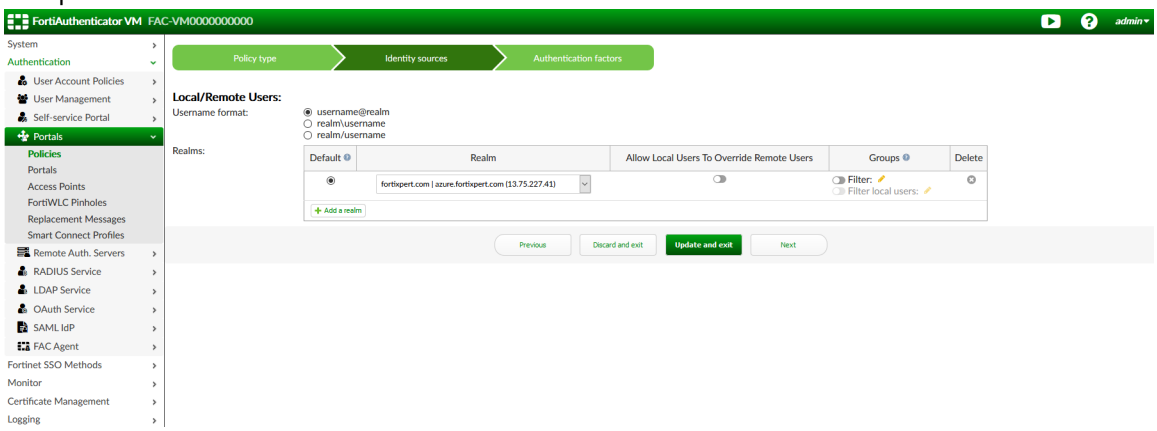
To create a self-service portal policy:

1. Go to *Authentication* > *Portals* > *Policies*. Select the *Self-Service Portal* option, and click *Create New*.
2. Under *Policy Type*, set the following and then click *Next*.
   a. **Name**: Enter a policy name, for example *SmartConnect*.
   b. **Description**: Enter an optional description for the policy.
   c. **URL**: Note this URL. This is the external captive portal redirection URL which must be added to the Onboarding SSID configured on the FortiGate/WLC later.
   d. **Portal**: Select the previously configured Smart Connect portal.



3. Under *Identity sources*, set the following and then click *Next*:
   a. **Username format**: username@realm.

b. **Realms**: In the dropdown box, select the LDAP realm associated with ldap.google.com, for example fortixpert.com.

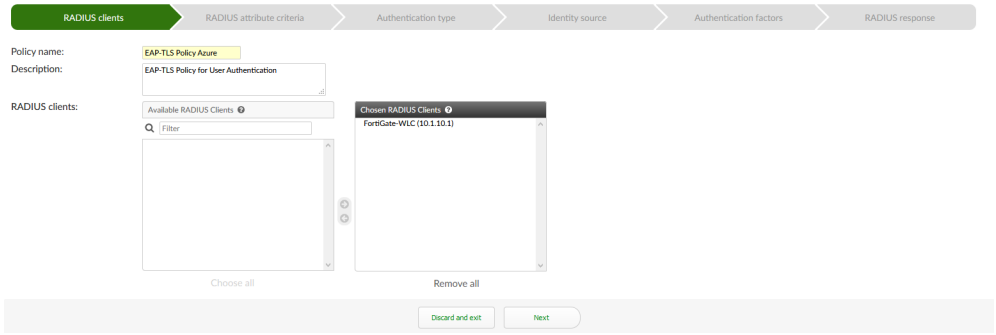


4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

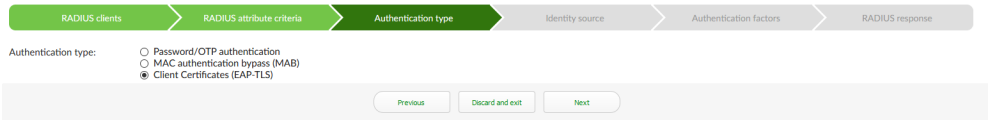
Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

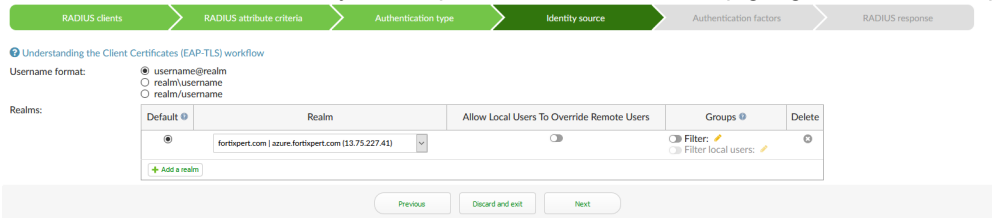
1. Go to *Authentication* > *RADIUS Service* > *Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy G Suite.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.



3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



5. Under *Identity source*, set the following and then click *Next*:
   a. **Username format**: Select your preferred format, for example username@realm.
   b. **Realms**: Select the realm that you set up to communicate with ldap.google.com, for example fortixpert.com.



6. Under *Authentication factors*, click *Next* without making changes.
7. Under *RADIUS response*, validate that the EAP-TLS response is as expected, and click *Save and exit*.

Option B - WiFi onboarding with Smart Connect and Azure

This section outlines how to configure the FortiAuthenticator to communicate with Microsoft Azure AD Directory Services via Secure Lightweight Directory Access Protocol

To configure WiFi Onboarding with Azure:

1. Configure Azure AD DS LDAPS integration on page 230
2. Configure Smart Connect and the captive portal on page 235
3. Configure RADIUS settings on FortiAuthenticator on page 238

Configure Azure AD DS LDAPS integration

This guide does not include information on how to provision Azure AD DS. Please refer to Microsoft's support site for instructions on how to do this.

To configure Azure AD DS LDAPS integration:

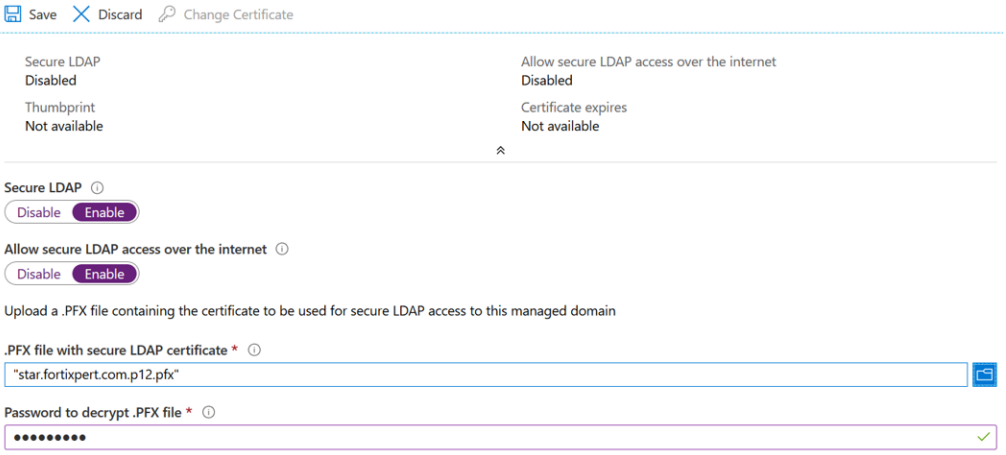
1. Provision the LDAPS connector in Azure AD DS on page 230
2. Provision the remote LDAP server on FortiAuthenticator on page 232

Provision the LDAPS connector in Azure AD DS

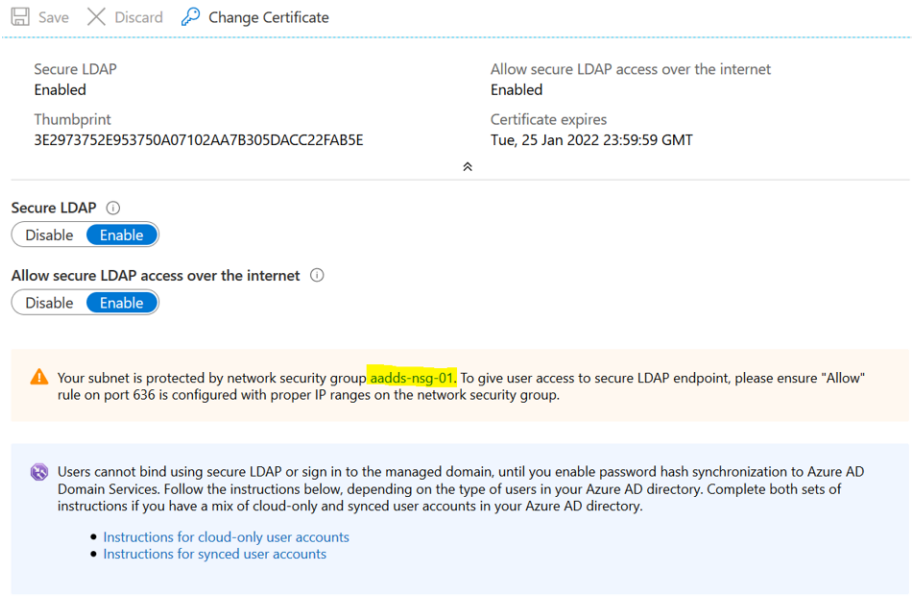
To provision the LDAP connector in Azure AD DS:

1. Login to the Azure admin portal using an Azure admin account.
2. Select *Active Directory Domain Services*.
3. Select *View*.
4. Select your AD DS instance, for example fortixpert.com.
5. Within the AD DS menu for your domain, select *Secure LDAP* under *Settings*.

6. In the Secure LDAP window, perform the following:
   a. Set *Secure LDAP* to *Enable*.
   b. Set *Allow secure LDAP access over the internet* to *Enable*.
   c. Upload your domain wildcard certificate, for example *.fortixpert.com, in .PFX format.
   d. Enter the password to decrypt the PFX file.



7. Select the *Save* button at the top of the page, and wait for Azure to configure Secure LDAP.
   This process takes approximately five minutes.
8. Once provisioning is complete, you must now allow inbound access for the secure LDAP protocol (port 636 to your AD DS instance.
9. Browse to the network security group linked in your Secure LDAP connector.
10. Select the network secure group link to access the network security group settings.
    You can follow the steps found on Microsoft's support website to enable user accounts for Azure AD DS. This is required for users to authenticate through Secure LDAP.



To create an Azure inbound firewall policy:

1. Within the network security group, go to *Settings* > *Inbound Security Rules*, and click *Add*.
2. In *Add inbound security rule*, set the following:
   a. **Source**: IP Address.
   b. **Source IP address/CIDR ranges**: Set as the IP address/range that the inbound request will be originating from.
   c. **Destination port ranges**: 636.
   d. **Name**: Enter the name, for example AllowSecureLDAP.
   e. **Description**: Add an optional description.
3. Leave all other settings as their default values, and click *Add*.

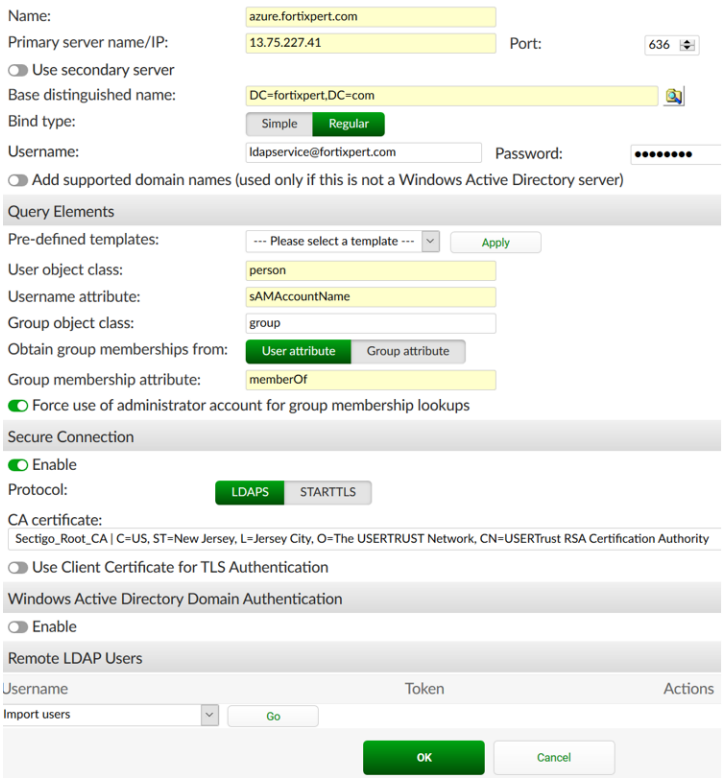
To obtain the LDAPS IP address:

1. Go to Azure AD Directory Services, and select the Azure domain.
2. Go to *Settings* > *Properties*. Note down the Secure LDAP external IP address.

Provision the remote LDAP server on FortiAuthenticator

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. In the *Create New LDAP Server* window, set the following:
   a. **Name**: Enter a name, for example azure.fortixpert.com.
   b. **Primary server name/IP**: Enter the Secure LDAP IP.
   c. **Bind type**: *Regular*.
   d. **Username/Password**: Enter a username and password that can access MS Azure DS to perform directory lookups.
   e. **Base distinguished name**: Leave blank.
3. In the *Query Elements* section, set the following:
   a. **Pre-defined templates**: Select *Microsoft Active Directory* and click *Apply*.
   b. **Force use of administrator account for group membership lookups**: Enabled.
4. In the *Secure Connection* section, set the following
   a. **Secure Connection**: Enabled.
   b. **Protocol**: *LDAPS*.
   c. **CA Certificate**: Select the Root CA certificate for the wildcard certificate that was uploaded to MS Azure to use with the Secure LDAP connector.
5. Select the lookup icon next to *Base distinguished name*. Choose the base DN for your user accounts, for example DC=fortixpert,DC=com. Click *OK*.

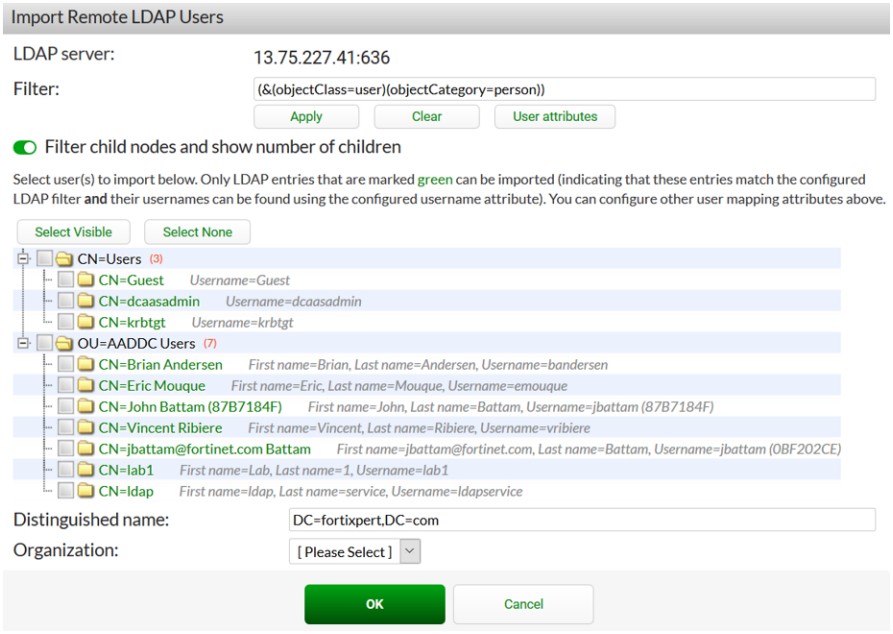


6. Click *OK* to save the remote LDAP server configuration.

To import remote user accounts:

1. Go to *Authentication* > *User Management* > *Remote Users*. Confirm *LDAP* is selected at the top of the page, and click *Import*.
2. Under *Import Remote LDAP User*, complete the following:
   a. **Remote LDAP Server**: Select the Azure remote LDAP server.
   b. **Action**: Select *Import users*, and click *Go* to view a list of users within your Azure directory.

c. Select the users you wish to be able to connect to the wireless network using their Azure based account.



3. Click *OK*.

To set up a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rule*, and click *Create New*.
2. Under *Create New Remote LDAP User Synchronization Rule*, set the following:
   a. **Name**: Enter a name, for example Azure_Remote_Sync.
   b. **Remote LDAP**: Select your Azure remote LDAP server.
   c. **Base distinguished name**: This setting can be left as the default, for example DC=fortixpert,DC=com.
3. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: Enable *None*.
   b. **Sync every**: Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.
4. Leave all other settings in their default states, and click *OK*.

To create a new realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Under *Create New Realm*, set the following:
   a. **Name**: Enter the realm name, for example fortixpert.com.
   b. **User source**: Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a Captive Portal using Smart Connect authenticating against MS Azure AD DS.

To configure Smart Connect and portals on FortiAuthenticator:

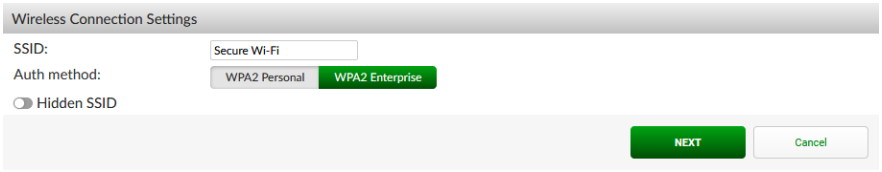
1. Create the Smart Connect profile on page 235
2. Create the captive portal on page 236
3. Create the self-service portal policy on page 237

Create the Smart Connect profile

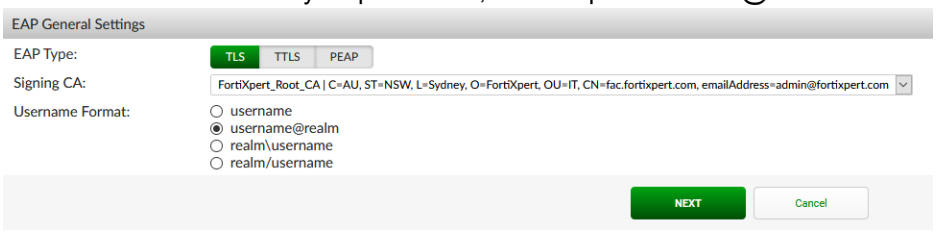
To create Smart Connect profiles:

1. Go to *Authentication* > *Portals* > *Smart Connect Profiles*, and click *Create New*.
2. Under *General Information*, enter a name for the profile, and click *Next*.

3. Under *Wireless Connection Settings*, set the following and then click *Next*.
   a. **SSID**: Enter your SSID name, for example Secure Wi-Fi.
   b. **Auth method**: *WPA2 Enterprise*.
   c. **Hidden SSID**: *Disabled*.

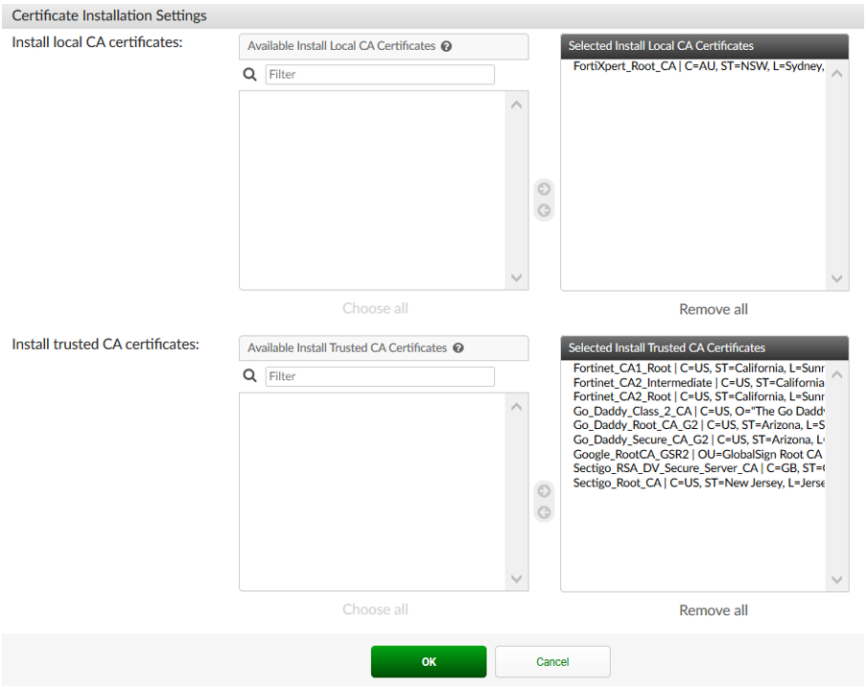


4. Under *EAP General Settings*, set the following and then click *Next*.
   a. **EAP Type**: *TLS*.
   b. **Signing CA**: Select the local Root CA configured earlier.
   c. **Username Format**: Select your preference, for example *username@realm*.



5. Under *Certificate Installation Settings*, set the following and then click *OK*.
   a. **Install local CA certificates**: Choose to install the local Root_CA certificate.
   b. **Install trusted CA certificates**: Choose to install any certificate that is required for all relevant certificate

chains to be fully trusted.

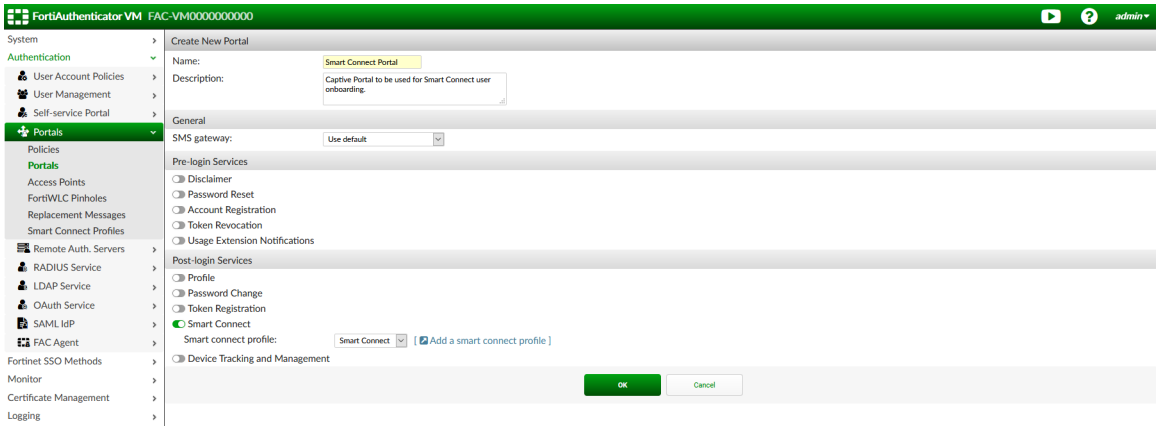


6. Select *OK* to complete the setup of the Smart Connect profile.

Create the captive portal

To create a captive portal:

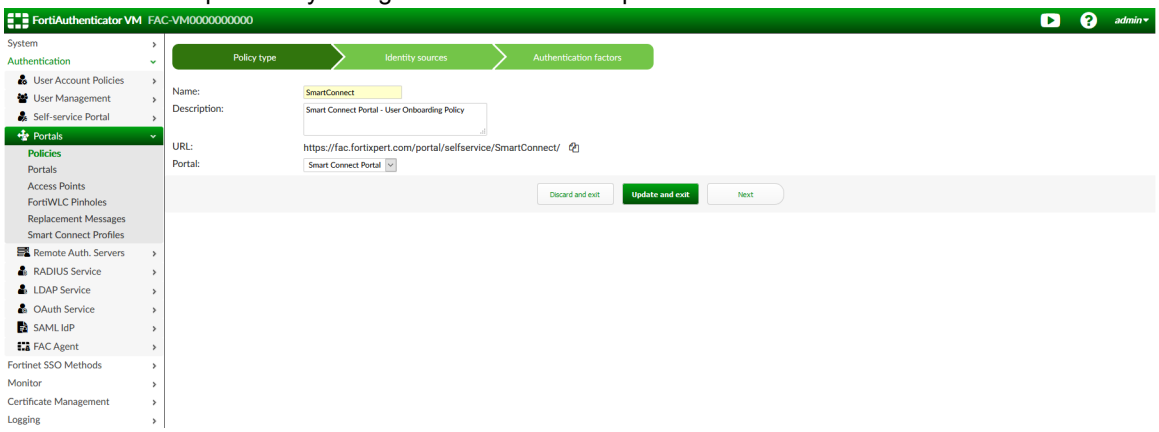
1. Go to *Authentication* > *Portals* > *Portals*, and click *Create New*.
2. Under *Create New Portal*, enter a name and optional description for the portal.
3. Under *Post-login services*, enable *Smart Connect* and select the previously configured Smart Connect profile from the dropdown.
4. Select *OK*.



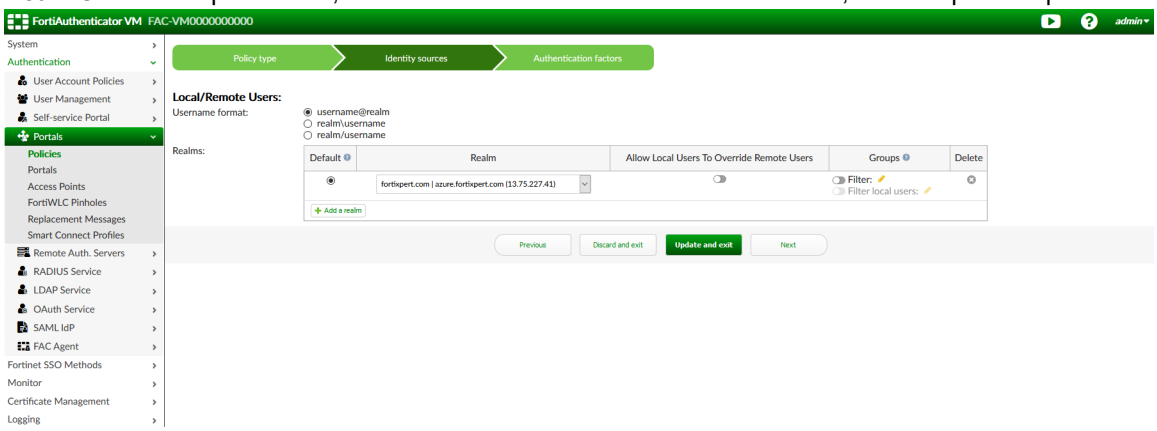
Create the self-service portal policy

To create a self-service portal policy:

1. Go to *Authentication* > *Portals* > *Policies*. Select the *Self-Service Portal* option, and click *Create New*.
2. Under *Policy Type*, set the following and then click *Next*.
   a. **Name**: Enter a policy name, for example *SmartConnect*.
   b. **Description**: Enter an optional description for the policy.
   c. **URL**: Note this URL. This is the external captive portal redirection URL which must be added to the Onboarding SSID configured on the FortiGate/WLC later.
   d. **Portal**: Select the previously configured Smart Connect portal.



3. Under *Identity sources*, set the following and then click *Next*:
   a. **Username format**: username@realm.
   b. **Realms**: In the dropdown box, select the LDAP realm associated with Azure, for example fortixpert.com.

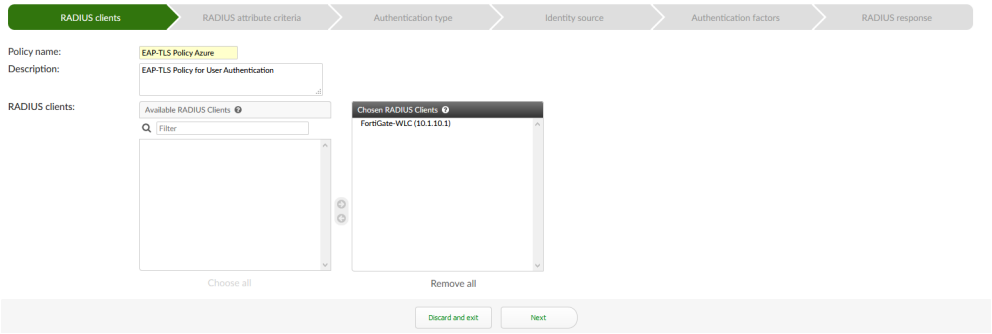


4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

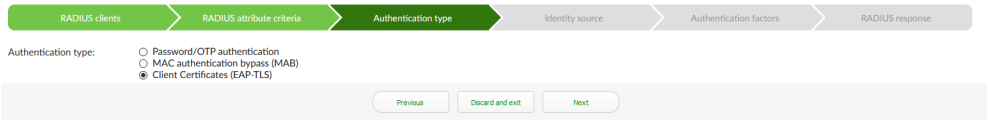
Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

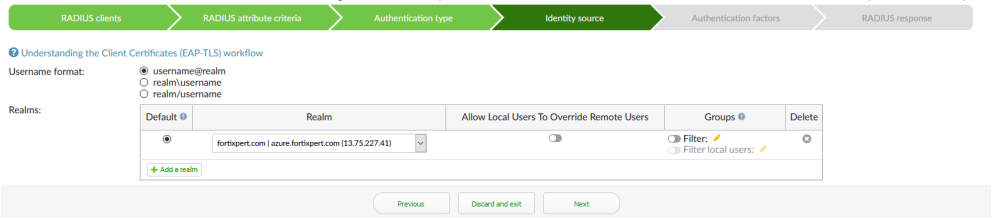
1. Go to *Authentication* > *RADIUS Service* > *Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy Azure.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.



3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



5. Under *Identity source*, set the following and then click *Next*:
   a. **Username format**: Select your preferred format, for example username@realm.
   b. **Realms**: Select the realm that you set up to communicate with Azure, for example fortixpert.com.



6. Under *Authentication factors*, click *Next* without making changes.
7. Under *RADIUS response*, validate that the EAP-TLS response is as expected, and click *Save and exit*.

FortiGate configuration

This section outlines the configuration required on FortiGate WLAC to provision an onboarding (Smart Connect enabled) WiFi network and a secure (WPA2 + EAP-TLS enabled) Wi-Fi network.

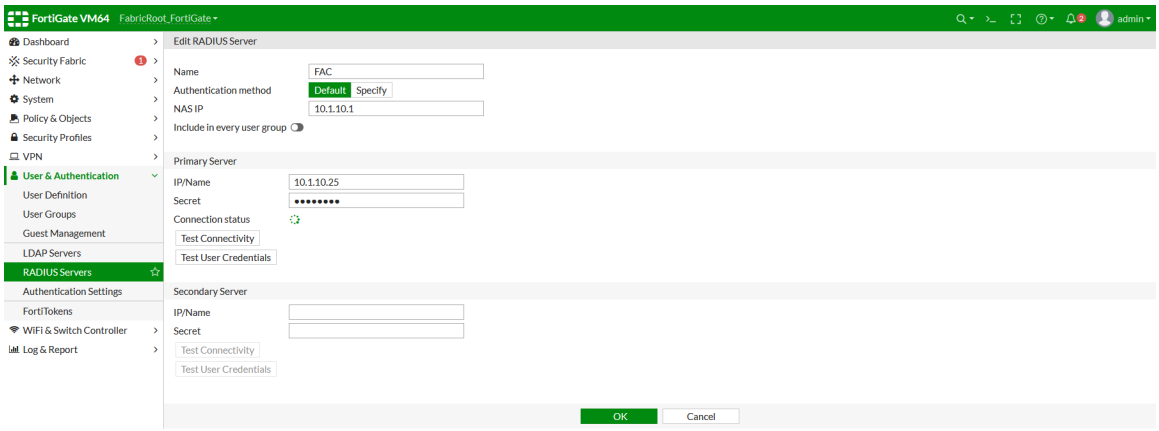
To configure the FortiGate:

1. Configure the RADIUS server on FortiGate on page 239
2. Create the user group for cloud-based directory user accounts on page 239
3. Provision the Onboarding and Secure WiFi networks on page 240

Configure the RADIUS server on FortiGate

To configure the RADIUS server:

1. In FortiGate, go to *User & Authentication* > *RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
   a. **Name**: Enter a name for the RADIUS server, for example FAC.
   b. **NAS IP**: Enter the Network Access Server (NAS) IP. This should ideally be the IP from the interface/VLAN FortiAuthenticator is on.
3. Under *Primary Server*, set the following:
   a. **IP/Name**: Enter the FortiAuthenticator IP address.
   b. **Secret**: Enter the secret matching the one configured on FortiAuthenticator.
4. Click *Test Connectivity* to test if the connection is correctly configured, and click *OK*.

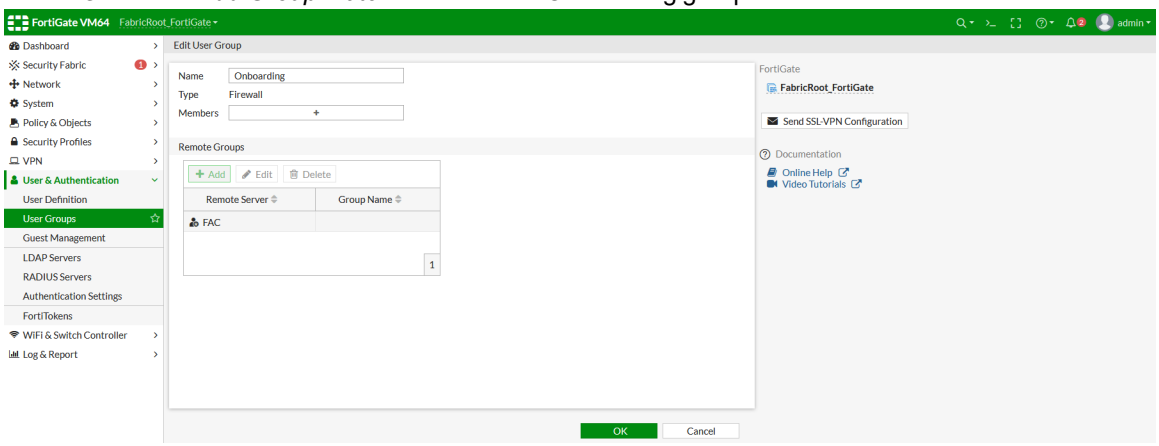


Create the user group for cloud-based directory user accounts

To create user groups:

1. Go to *User & Authentication* > *User Groups*, and click *Create New*.
2. Configure the following settings:
   a. **Name**: Configure a name, for example Onboarding.
   b. **Type**: Firewall.
   c. **Remote Groups**: Select *Add*. Within the Add Group Match window, select FortiAuthenticator as the remote server from the dropdown box.
   d. **Groups**: Any.

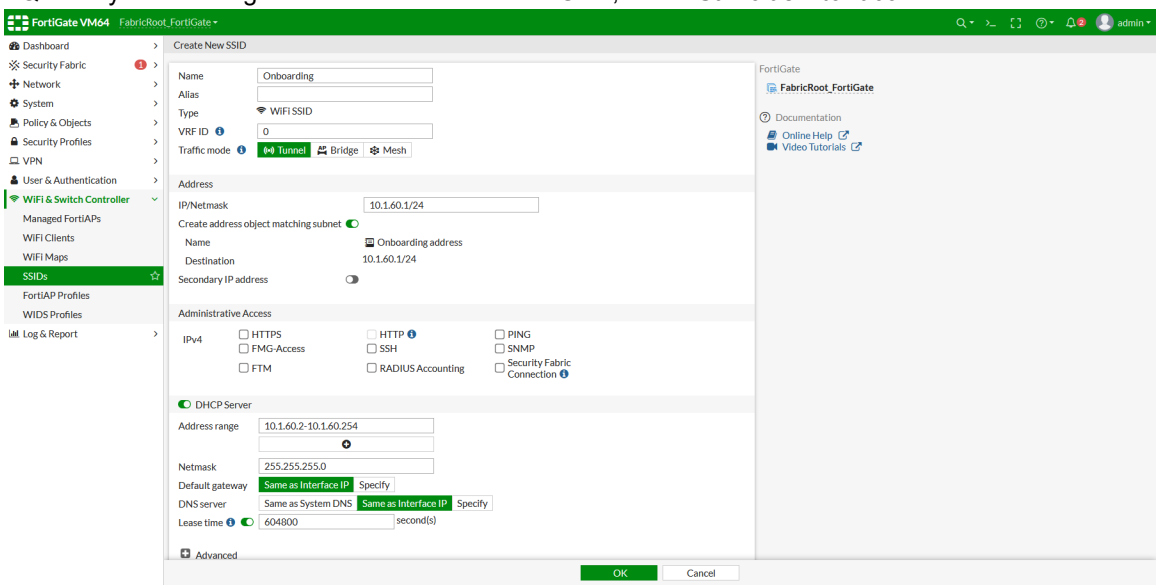
3. Select *OK* on the *Add Group Match* window. The Onboarding group is now created.



Provision the Onboarding and Secure WiFi networks

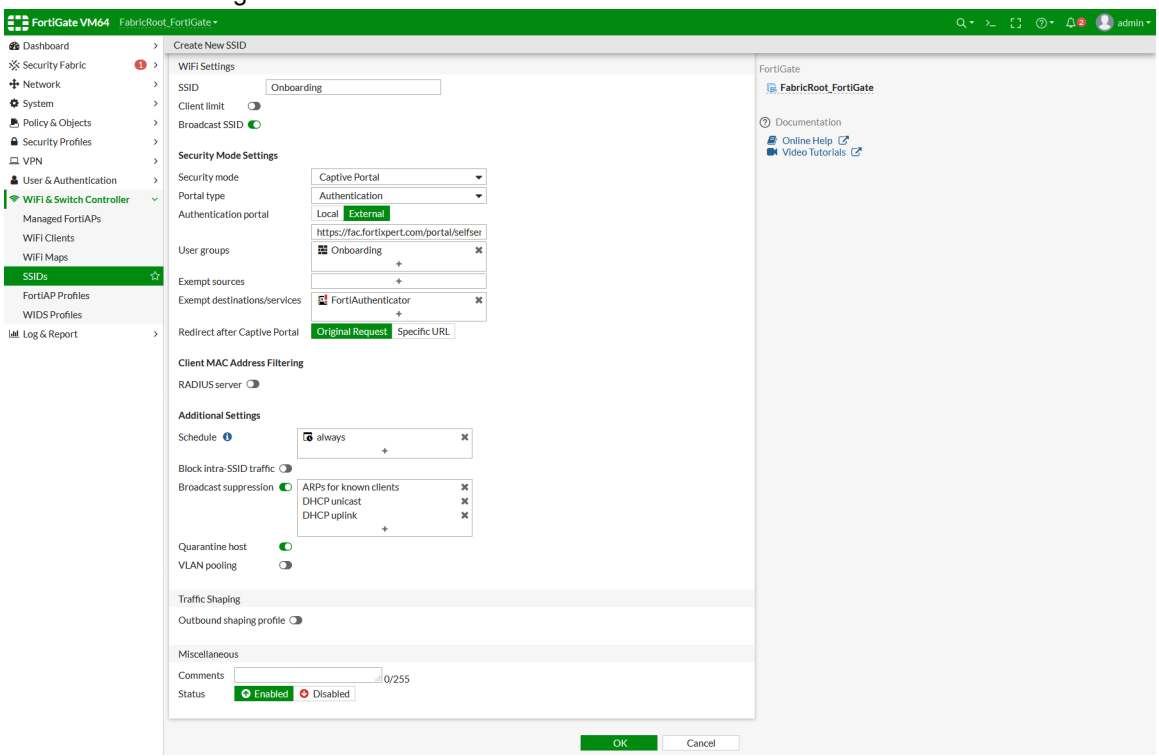
To provision the Smart Connect enabled "Onboarding" SSID:

1. Go to *Wi-Fi & Switch Controller* > *SSID*, and click *Create New*.
2. Under *Create New SSID*, set the following:
   a. **Profile name**: Enter a name for the profile, for example Onboarding.
   b. **Traffic mode**: *Tunnel*.
3. Under *Address*, set the following:
   a. **IP/Netmask**: Enter the interface IP address for the Onboarding SSID.
4. Under *DHCP Server*, enable the DHCP Server setting and set the following:
   a. Leave *Address range*, *Netmask*, *Gateway*, and *Lease time* in their default states.
   b. **DNS server**: Select *Same as Interface IP* or specify a local DNS server that can resolve your FortiAuthenticator FQDN. If you are using the DNS database on FortiGate, select *Same as Interface IP*.



5. Under *Network*, leave the *Decide detection* setting enabled.

6. Under *WiFi Settings*, set the following:
   a. **SSID**: Enter the SSID, for example Onboarding.
   b. **Security mode**: *Captive Portal*.
   c. **Portal type**: *Authentication*.
   d. **Authentication portal**: Select *External*, and enter the FortiAuthenticator Smart Connect portal redirection URL obtained when configuring Smart Connect on FortiAuthenticator.
   e. **User groups**: Select the previously configured user group, for example Onboarding.
   f. **Exempt destinations/services**: Select FortiAuthenticator.
   g. Leave all other settings as their default state.

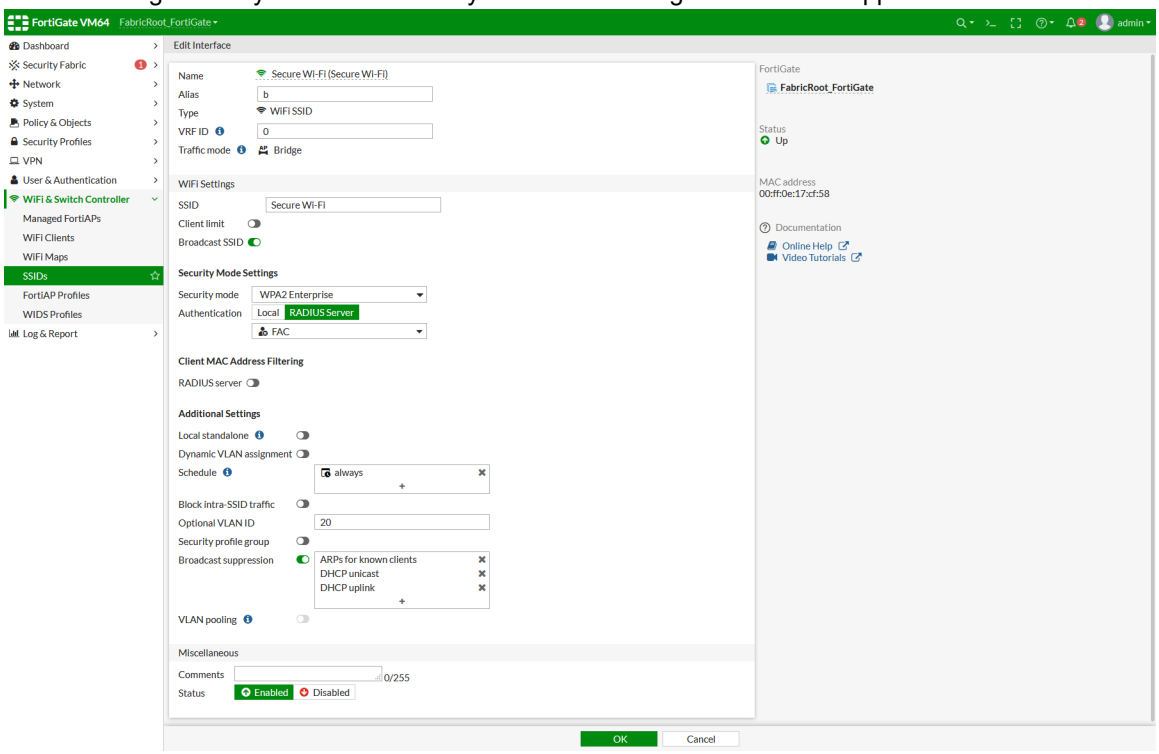


7. Click *OK*.

To provision the "Secure Wi-Fi" network:

1. Go to *WiFi & Switch Controller* > *SSID*, and click *Create New*.
2. Configure the following settings:
   a. **Profile name**: Enter a profile name, for example Secure Wi-Fi.
   b. **Traffic mode**: *Bridge*.
   c. **SSID**: Enter the SSID name, for example Secure Wi-Fi.
   d. **Security mode**: *WPA2 Enterprise*.
   e. **Authentication**: Choose *RADIUS Server*, and select the FortiAuthenticator.

f. **Optional VLAN ID**: This setting is optional and can be configured if WiFi traffic needs to be tagged by the AP to a VLAN configured on your local switch. Dynamic VLAN assignment is also supported.



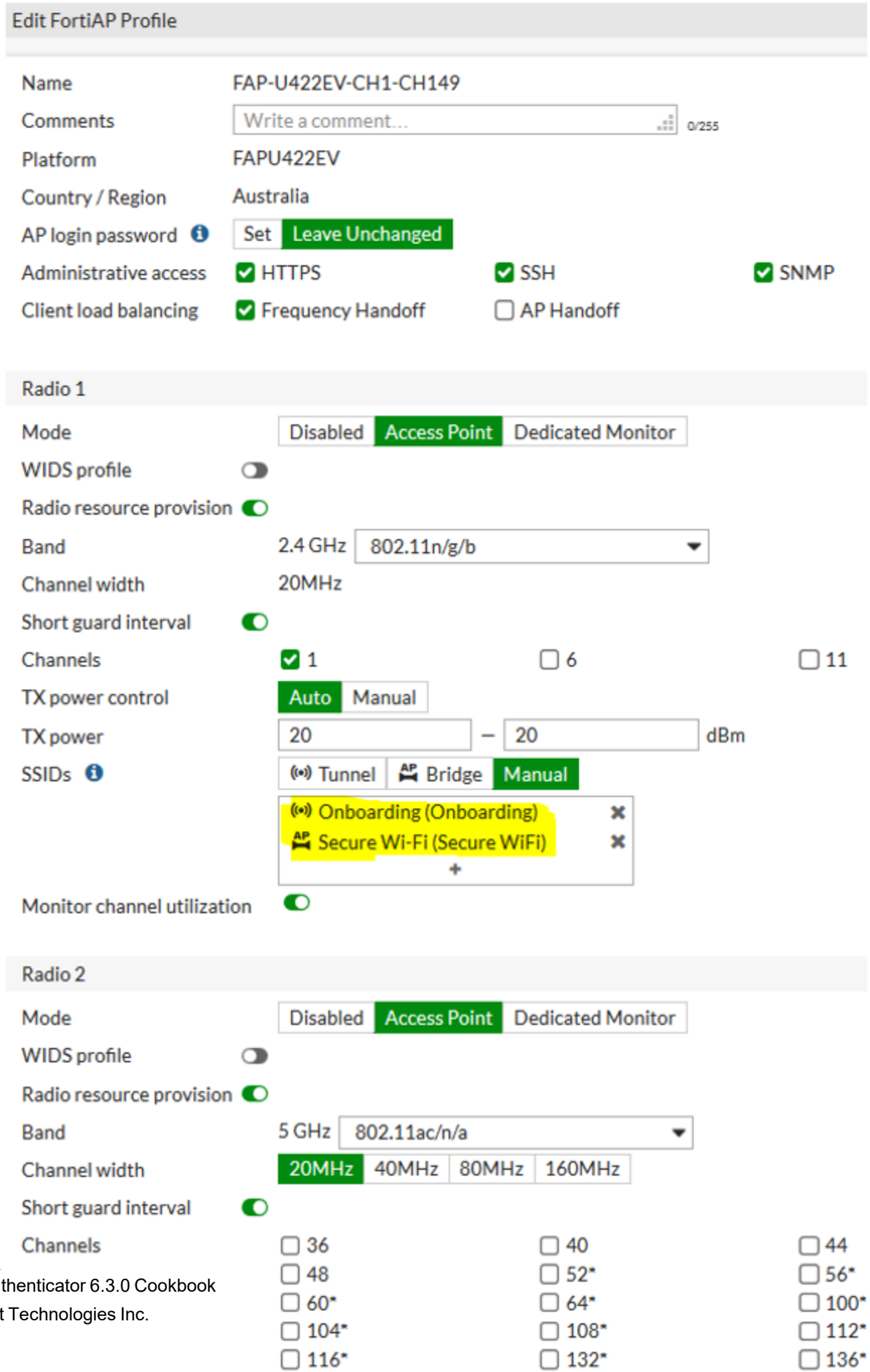
3. Click *OK*.

To assign SSIDs to FortiAP profiles:

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles*.
2. Select the relevant AP profile(s) and assign the previously created SSIDs (Onboarding and Secure Wi-Fi) to the

AP radio interfaces.

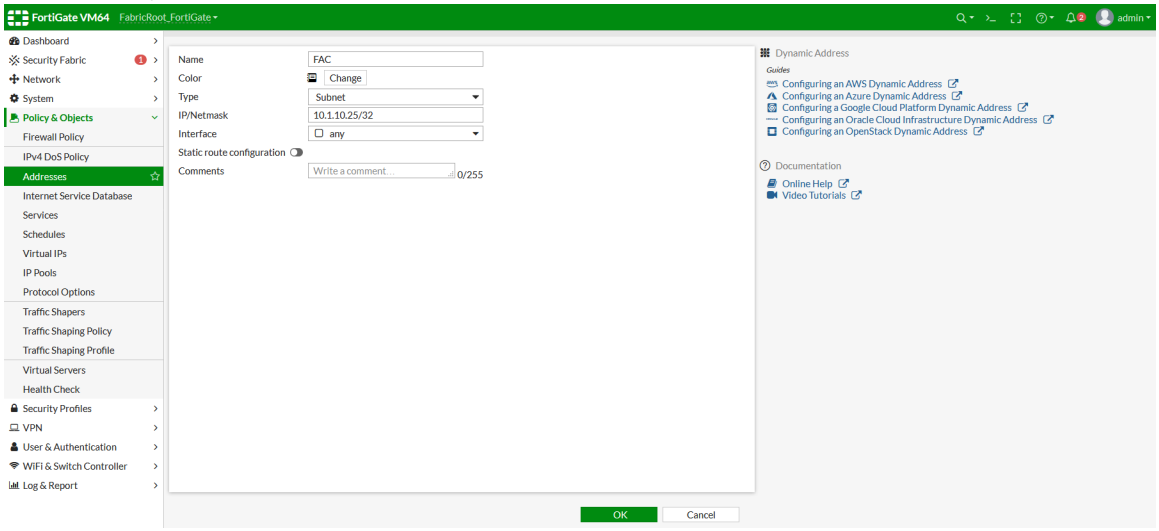
3. Confirm the SSIDs are broadcasting and can be seen by WiFi enabled devices.


Edit FortiAP Profile
Name
FAP-U422EV-CH1-CH149
Comments
Write a comment...
0/255
Platform
FAPU422EV
Country / Region
Australia
AP login password
Set
Leave Unchanged
Administrative access
HTTPS
SSH
SNMP
Client load balancing
Frequency Handoff
AP Handoff
Radio 1
Mode
Disabled
Access Point
Dedicated Monitor
WIDS profile
Radio resource provision
Band
2.4 GHz
802.11n/g/b
Channel width
20MHz
Short guard interval
Channels
1
6
11
TX power control
Auto
Manual
TX power
20
20
dBm
SSIDs
Tunnel
Bridge
Manual
Onboarding (Onboarding)
Secure Wi-Fi (Secure WiFi)
Monitor channel utilization
Radio 2
Mode
Disabled
Access Point
Dedicated Monitor
WIDS profile
Radio resource provision
Band
5 GHz
802.11ac/n/a
Channel width
20MHz
40MHz
80MHz
160MHz
Short guard interval
Channels
36
40
44
48
52*
56*
60*
64*
100*
104*
108*
112*
116*
132*
136*

4. Click *OK*.

To create a new FortiAuthenticator object to use with firewall policies:

1. Go to *Policy & Objects* > *Addresses*, and click *Create New* > *Address*.
2. Configure the following settings:
   a. **Name**: Enter a name, for example FAC.
   b. **Type**: *Subnet*.
   c. **IP/Netmask**: The FortiAuthenticator IP address.
   d. **Interface**: *any*.

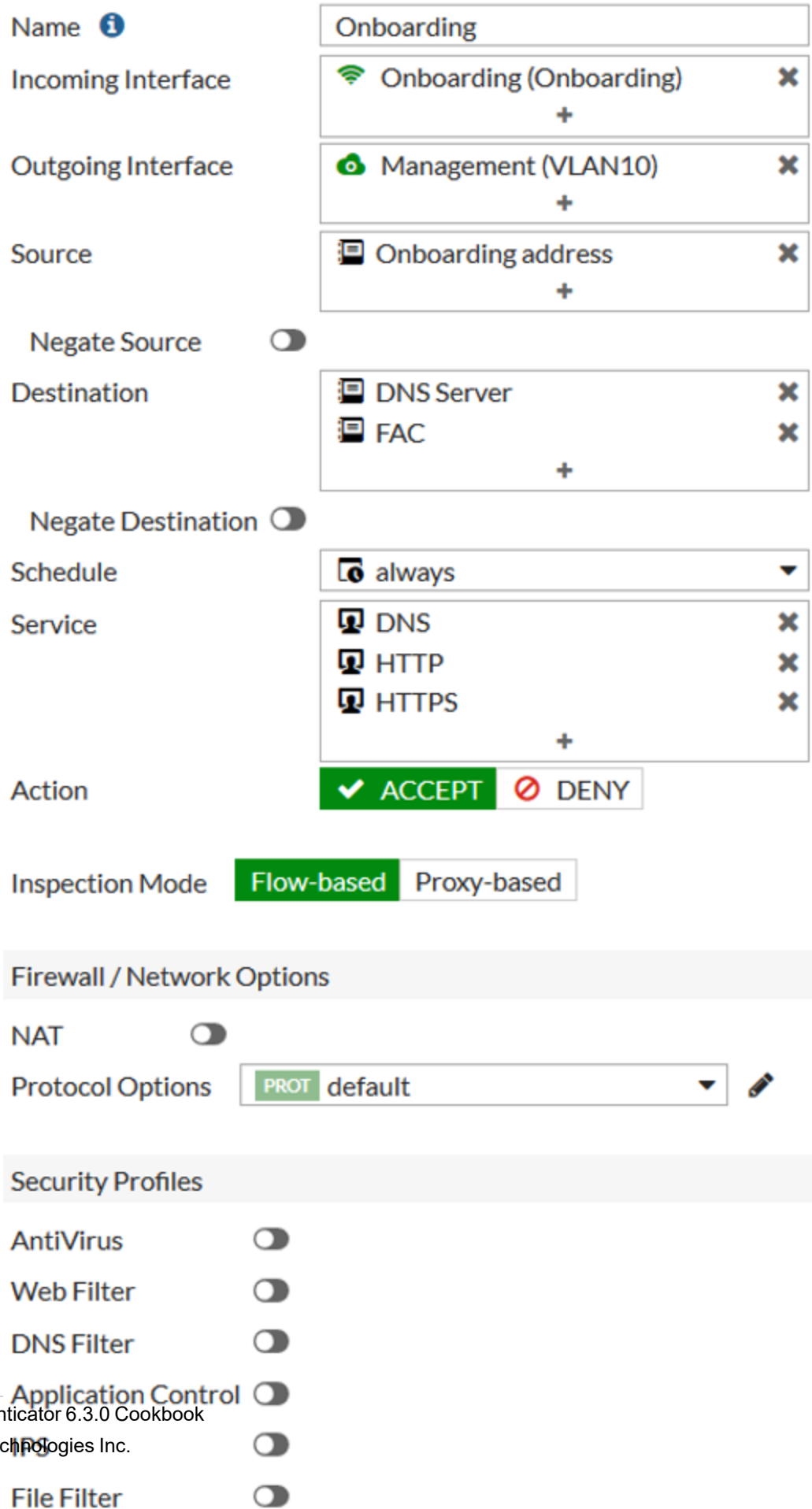


3. Click *OK*.

To create a firewall policy for the Onboarding SSID:

1. Go to *Policy & Objects* > *Firewall Policy*, and click *Create New*.
2. On the *New Policy* page, set the following:
   a. **Name**: Enter a name, for example Onboarding Policy.
   b. **Incoming Interface**: Select the Onboarding SSID.
   c. **Outgoing Interface**: Select the Management VLAN.
   d. **Source**: Select *all* or the Onboarding address subnet range.
   e. **Destination**: Select FortiAuthenticator and the DNS server if you are using a third party DNS server.
   f. **Service**: *DNS*, *HTTP*, and *HTTPS*.
   g. Under *Advanced*, enable the *Exempt from Captive Portal* option.
   When using a FortiOS version earlier than 6.4.1, you can enable this setting in the CLI with the command `set`

```
captive-portal-exempt enable.
```


Name
Onboarding
Incoming Interface
Onboarding (Onboarding)
Outgoing Interface
Management (VLAN10)
Source
Onboarding address
Negate Source
Destination
DNS Server
FAC
Negate Destination
Schedule
always
Service
DNS
HTTP
HTTPS
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
Protocol Options
PROT
default
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
IPS
File Filter

3. Click *OK*.

Results

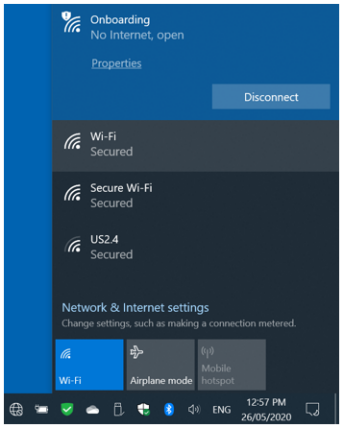
You can now connect your device to the Onboarding SSID and proceed with the Smart Connect onboarding process:

- Smart Connect Windows device onboarding process on page 249
- Smart Connect iOS device onboarding process on page 251

Smart Connect Windows device onboarding process

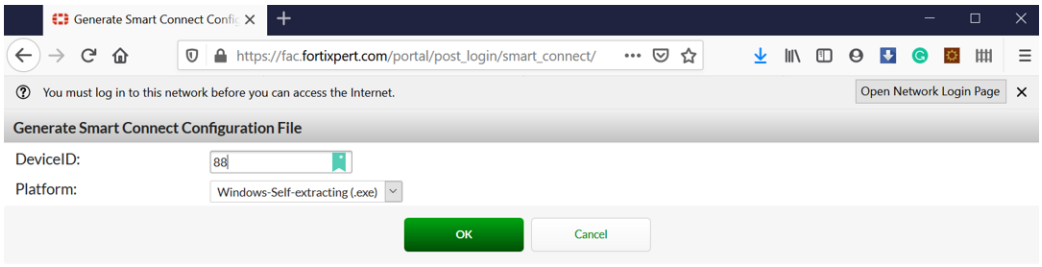
To onboard a Windows device:

1. On your Windows device, connect to the Onboarding WiFi network.



   The FortiAuthenticator login screen is displayed.
2. Enter either your G Suite or Azure login credentials, and select *Login*.
   Once logged in, select *Smart Connect*.

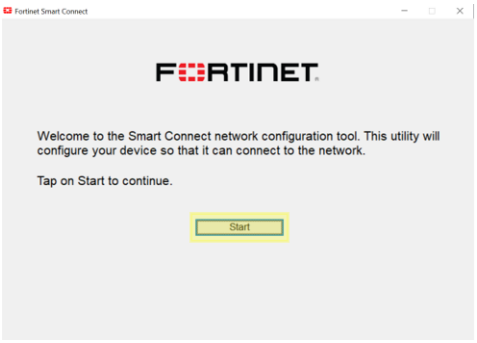
3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



A *SmartConnect_UserName.exe* file will be made available. Save this file.

4. Run the *SmartConnect_UserName.exe* file.
If the Microsoft Defender warning message appears, click *More info* > *Run anyway*. If the User Account Control warning appears, click *Yes*.
The Fortinet Smart Connect network configuration tool will now run.

5. Select *Start*.



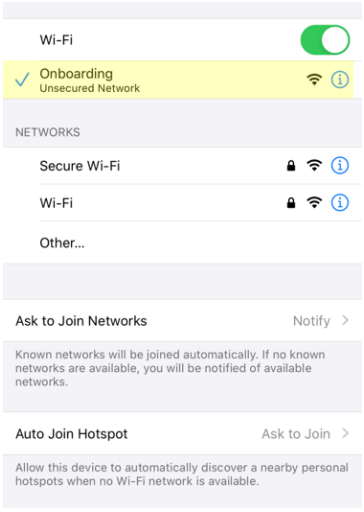
Your device will now be provisioned with the wireless network information and certificates in order to connect to the Secure Wi-Fi SSID.

6. Once provisioning is complete, click *Connect*. Your device will now connect to the Secure Wi-Fi network using WPA2 and EAP-TLS.
You may wish to forget the Onboarding network to prevent your device from automatically connecting to it in the future.

Smart Connect iOS device onboarding process

To onboard an iOS device:

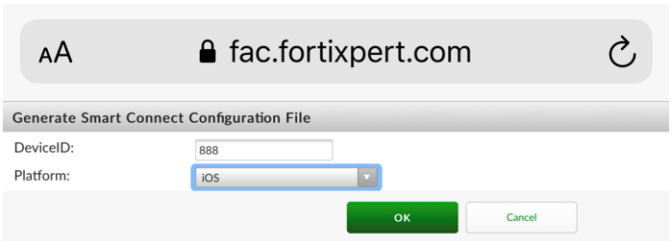
1. On the iOS device, connect to the Onboarding WiFi network.



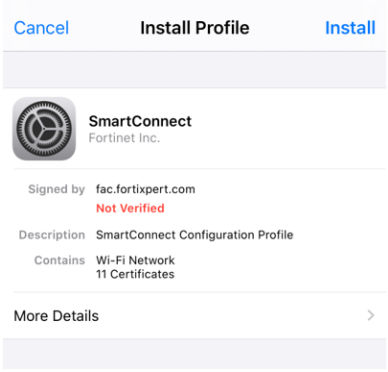
   The FortiAuthenticator login screen is displayed.

2. Enter either your G Suite or Azure login credentials, and select *Login*.
   Once logged in, select *Smart Connect*.

3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



4. When prompted, download the configuration profile.
5. In *Settings*, select *Profile Downloaded*.
6. Select *Install* within the SmartConnect Install Profile. Depending on your device setup, you may be prompted to enter your device passcode/password.



7. On the warning screen, select *Install* to install any root certificates included within the profile. Once the installation is finished, click *Done*.
8. In *Settings*, select the information icon next to the Onboarding WiFi network and select *Forget this Network*. Once the network has been forgotten, the device will automatically connect to the Secure Wi-Fi network.

www.fortinet.com